Characterizing contextual equivalence in calculi with passivation

Sergueï Lenglet, Alan Schmitt, Jean-Bernard Stefani

Characterizing Contextual Equivalence in Calculi with Passivation

Sergueï Lenglet[a], Alan Schmitt[b], Jean-Bernard Stefani[b]

[a] *Université Joseph Fourier, Grenoble, France*
[b] *INRIA, Grenoble, France*

Abstract

We study the problem of characterizing contextual equivalence in higher-order languages with passivation. To overcome the difficulties arising in the proof of congruence of candidate bisimilarities, we introduce a new form of labelled transition semantics together with its associated notion of bisimulation, which we call *complementary semantics*. Complementary semantics allows to apply the well-known Howe's method for proving the congruence of bisimilarities in a higher-order setting, even in the presence of an early form of bisimulation. We use complementary semantics to provide a coinductive characterization of contextual equivalence in the HOπP calculus, an extension of the higher-order π-calculus with passivation, obtaining the first result of this kind. We then study the problem of defining a more effective variant of bisimilarity that still characterizes contextual equivalence, along the lines of Sangiorgi's notion of *normal bisimilarity*. We provide partial results on this difficult problem: we show that a large class of test processes cannot be used to derive a normal bisimilarity in HOπP, but we show that a form of normal bisimilarity can be defined for HOπP without restriction.

1. Introduction

1.1. Characterizing contextual equivalence in higher-order concurrent languages

A natural notion of program equivalence in concurrent languages is a form of contextual equivalence called *barbed congruence*, introduced by Milner and Sangiorgi [31]. Roughly, given an operational semantics defined by means of a small-step reduction relation, two processes are barbed congruent if they have the same reductions and the same observables (or *barbs*), under any context.

The definition of barbed congruence, however, is impractical to use in proofs because of its quantification on contexts. An important question, therefore, is to find more effective characterizations of barbed congruence. A powerful method

Email addresses: serguei.lenglet@gmail.com (Sergueï Lenglet), alan.schmitt@inria.fr (Alan Schmitt), jean-bernard.stefani@inria.fr (Jean-Bernard Stefani)

for proving program equivalence is the use of coinduction with the definition of an appropriate notion of *bisimulation*. The question of characterizing barbed congruence to enable the use of coinduction becomes that of finding appropriate bisimulation relations such that their resulting behavioral equivalences, called *bisimilarities*, are *sound* (i.e., included in) and *complete* (i.e., containing) with respect to barbed congruence.

For first-order languages, such as CCS or the π-calculus, the behavioral theory and the associated proof techniques, e.g., for proving congruence, are well developed [39]. Characterizing contextual equivalence in these languages, i.e., finding a bisimilarity relation that is both sound and complete with respect to barbed congruence, is a reasonably well understood proposition.

The situation is less satisfactory for higher-order concurrent languages. Bisimilarity relations that coincide with barbed congruence have only been given for some higher-order concurrent languages. They usually take the form of *context bisimilarities*, building on a notion of *context bisimulation* introduced by D. Sangiorgi for a higher-order π-calculus, HOπ [37]. Context bisimilarity has been proven to coincide with contextual equivalence for higher-order variants of the π-calculus: Sangiorgi's HOπ [36, 37, 20], a concurrent ML with local names [19], a higher-order distributed π-calculus called SafeDpi [16], Mobile Ambients [29], and some of Mobile Ambients's variants such as Boxed Ambients [5]. A sound but incomplete form of context bisimilarity has been proposed for the Seal calculus [10]. For the Homer calculus [14], strong context bisimilarity is proven sound and complete, but weak context bisimilarity is not complete. A sound and complete context bisimilarity has been defined for the Kell calculus [41], but for the strong case only.

Context bisimilarity is not entirely satisfactory, however. Its definition still involves quantification on processes (or on *abstractions* and *concretions*, following Milner's terminology [30], that can be understood, respectively, as receiving processes and emitting processes).[1] For this reason, Sangiorgi has introduced in his study of HOπ [37] an alternative form of bisimulation, called *normal bisimulation*, that replaces the universal quantification on processes in the input and output clauses in the definition of context bisimulation with a single test process.[2] To the best of our knowledge, the only higher-order concurrent language for which normal bisimilarity has been defined and proved to coincide

[1] Despite this quantification on processes, the use of context bisimulation as a proof technique is still an improvement over the direct use of barbed congruence, as argued in [29]. Removing this quantification would pave the way to automated proof support.

[2] For instance, the definition of an early strong contextual bisimulation $\mathcal{R}$ in HOπ has the following *input clause*:

- for all $P \xrightarrow{a} F$, $\forall C$, $\exists F'$ such that $Q \xrightarrow{a} F'$ and $F \bullet C \; \mathcal{R} \; F' \bullet C$

This input clause requires to find a matching transition for all emitting processes (actually concretions) C. The corresponding clause in the definition of strong normal bisimilarity takes the form:

- for all $P \xrightarrow{a} F$, $\exists F'$ such that $Q \xrightarrow{a} F'$ and $F \bullet C_0 \; \mathcal{R} \; F' \bullet C_0$

where C_0 is a fixed (up to the choice of a fresh name) emitting test process (concretion).

with context bisimilarity is HOπ and its typed variant [36, 37, 20].

1.2. Process calculi with passivation

The difficulties in characterizing contextual equivalence are particularly acute in calculi featuring *process passivation*, such as the Homer calculus, the Kell calculus, and, to some extent, the Seal calculus.

Let us motivate first our interest in higher-order languages with strong process mobility and process passivation. Strong process mobility refers to the possibility of moving a running process from one locus of computation (or *locality*) to another. This feature typically occurs in languages or calculi intended for distributed programming such as the Join calculus [27], Mobile Ambients [8], or Nomadic Pict [44]. Process passivation refers to the ability to suspend the execution of a named running process and to pass around the suspended process, typically as a higher-order parameter in messages. This capability is featured in the Homer calculus [14], the M-calculus [40], and the Kell calculus [41]. Passivation actually subsumes strong mobility, as discussed in [41], since strong mobility amounts to a sequence of passivation, transfer of the suspended process between localities, and reactivation. Strong mobility is a linear operation that moves a computation from one locality to another, whereas passivation may be non-linear: a passivated process can be reactivated several times. The Seal calculus [10] provides an intermediate form, with a combined migrate and replicate (and hence non-linear) operation.

Strong mobility is one of several paradigms for mobile code. It has been introduced as a primary feature in several languages, including Obliq [7], Nomadic Pict [44], and JoCaml [12]. It potentially allows interesting performance and design trade-offs [9, 13], and its use can be compelling in certain application areas such as network and distributed system management [3]. Process passivation provides basic support for dynamic reconfiguration: with passivation, named parts of a system can be replaced during execution. Dynamic reconfiguration is useful to support patches and system updates while limiting system downtime and increasing availability; to support fault recovery and fault tolerance by providing a basic mechanism for checkpointing computations and replicating them; and to support adaptive behaviors, whereby a system changes its configuration to adapt to varying operating conditions, with the aim of improving performance and/or dependability. A form of process passivation has been introduced in the Acute programming language [42] for the same reasons. There, it is called *thunkification* and applies to designated groups of threads.

In this paper, we work with the HOπP calculus, a minimal extension of HOπ with passivation. An example of process passivation in HOπP is given by the following reduction:

$$a[P] \mid a(X)Q \longrightarrow Q\{P/X\}$$

where $a[P]$ is a locality named a that contains a process P, and $a(X)Q$ is a receiver process. The passivation above removes the locality a, and passes process P as an argument to the receiver process $a(X)Q$. A locality $a[\ ]$ is an execution context and is transparent: if P can evolve into P' (i.e., $P \longrightarrow P'$),

then we have $a[P] \longrightarrow a[P']$. Also, if P can emit a message, then $a[P]$ can also emit the same message. This form of passivation in HOπP is a simplification of the passivation constructs present in the Kell calculus and in the Homer calculus. In particular, we eschew the use of join patterns of the Kell calculus, and of communication paths of the Homer calculus.

1.3. Contributions

This paper contributes to the study of the interrelated issues of proving the congruence of bisimilarity relations and of characterizing barbed congruence in higher-order concurrent languages,[3] notably those featuring strong process mobility and process passivation capabilities such as the Seal calculus, the Homer calculus, or the Kell calculus. Specifically, this paper makes two sets of contributions: positive ones and negative ones.

On the positive side, we develop a new form of labelled transitions semantics and its associated bisimulation, which we call *complementary semantics*, that is devised to overcome the difficulties that appear when trying to apply Howe's method in proving the congruence and soundness of bisimulation relations defined in an early style. Howe's method is a systematic technique for proving the congruence of bisimilarity relations [18, 1, 15]. Unfortunately, Howe's method is originally well suited for bisimulations that are defined in both a late and a delay style, either of which generally breaks the correspondence with contextual equivalence.[4] In their work on the Homer calculus, Godskesen and Hildebrandt have managed to extend Howe's method to a version of context bisimulation in an input-early style [14], but the resulting weak bisimilarity is not complete with respect to weak barbed congruence. To our knowledge, our work is the first one to exploit Howe's method to prove congruence with bisimulation relations defined in an early style. We then show that complementary semantics and complementary bisimilarity can be used successfully to characterize barbed congruence in HOπP, a minimal extension of (the second-order fragment of)

[3] Proving the congruence of a candidate bisimilarity is typically the key step in proving its soundness with respect to barbed congruence.

[4] The early or late style of a bisimulation relation refers to the order of certain quantifications in its definition. For instance, the definition of an early strong contextual bisimulation $\mathcal{R}$ in HOπ has the following two clauses:

- *input clause:* for all $P \xrightarrow{a} F$, $\forall C$, $\exists F'$ such that $Q \xrightarrow{a} F'$ and $F \bullet C \mathcal{R} F' \bullet C$;
- *output clause:* for all $P \xrightarrow{\overline{a}} C$, $\forall F$, $\exists C'$ such that $Q \xrightarrow{\overline{a}} C'$ and $F \bullet C \mathcal{R} F \bullet C'$.

The late variant of strong contextual bisimulation can be obtained by exchanging the order of the quantifications $\forall C, \exists F'$ in the input clause, and of the quantifications $\forall F, \exists C'$ in the output clause. In other words, the "early" and late styles in a contextual bisimulation game define when a test process is selected with respect to the move of the adversary: in the early style, a test process C or F is selected *before* (hence the term *early*) the adversary has to pick a matching move F' or C'.

The qualifier *delay* is used in relation with weak forms of contextual bisimulations. In the definition of a delay bisimulation, internal actions are allowed before but not after a visible action.

Sangiorgi's HOπ with passivation. This is also, to our knowledge, the first result of its kind.

On the negative side, we show that we we cannot readily exploit Sangiorgi's notion of normal bisimulation to derive more effective forms of bisimilarities than contextual or complementary bisimilarity for concurrent higher-order languages with process passivation. Specifically, we show that a large class of test processes cannot be used to define for HOπP a notion of normal bisimilarity similar to the one defined for HOπ. The difficulty seems to be linked to the interplay between passivation and restriction. Indeed, we show that a form of normal bisimilarity can be defined for HOP, a calculus which is essentially HOπP without restriction, and that it coincides with barbed congruence.

1.4. Organization of the paper

The paper is organized as follows. In Section 2, we recall the main results on HOπ, the higher-order π-calculus. We then introduce the HOπP calculus, a minimal extension of HOπ with passivation. In Section 3, we review two existing techniques for proving congruence of context bisimilarities: the technique used in the proof of congruence of strong context bisimilarity in the Kell calculus, and Howe's method. We explain why the Kell calculus method fails when trying to prove the congruence of weak context bisimilarities, and why Howe's method fails when using early context bisimilarities. In Section 4, we present our notion of complementary semantics, using the HOπ calculus as an example. In Section 5, we present a complementary semantics for the HOπP calculus, and we prove that in HOπP complementary bisimilarity coincides with barbed congruence. In Section 6, we present counter examples that show that Sangiorgi's notion of normal bisimilarity, which he developed initially for HOπ, cannot be readily applied to HOπP. In Section 7, we show that a form of normal bisimilarity can be defined for a sublanguage of HOπP called HOP, which is essentially HOπP without restriction, and that normal bisimilarity coincides with barbed congruence in HOP. Section 8 discusses related work. Section 9 concludes the paper and discusses future work. Appendix A gives the proofs of the main theorems regarding the complementary semantics of HOπP (Section 5), namely the relation between context and complementary semantics, and the soundness of completeness results of weak complementary bisimilarity with respect to barbed congruence. Appendix B elaborates on the finite processes counter-examples given in Section 6, and Appendix C contains the proofs regarding the normal bisimilarity of HOP (Section 7).

This paper refines and extends previous papers by the authors [26, 25]. The HOπP calculus was first introduced in [26]. The results presented in Section 5 were given in [25] with only proof hints. The results presented in Section 7 and in Section 6.1 were given in [26] with only proof hints. The material in Sections 3, 4, 6.2, and 6.3 is new.

$$P ::= \mathbf{0} \;\mid\; X \;\mid\; P \mid P \;\mid\; a(X)P \;\mid\; \overline{a}\langle P\rangle P \;\mid\; \nu a.P \;\mid\; !P$$

Figure 1: Syntax of the Higher Order π-Calculus

2. The HOπ and HOπP calculi

We recall in this Section previous results on HOπ, the higher order π-calculus. We also introduce HOπP, an extension of HOπ with a passivation operator.

2.1. The Syntax and Contextual Semantics of HOπ

The higher order π-calculus [37] is a variant of the π-calculus with higher-order communication: the communication of names of the standard π-calculus is replaced by the communication of processes.

We now state some conventions on notations. We let $a, b, \ldots$ range over names, $\overline{a}, \overline{b}, \ldots$ range over conames, and $X, Y, \ldots$ range over process variables. We write $\widetilde{x}$ for a set $\{x_1, \ldots, x_n\}$. Finally, we let γ range over names and conames.

The syntax of the calculus is given in Figure 1. Terms include the inactive process $\mathbf{0}$, process variables X, parallel composition of processes $P \mid P$, input prefixing $a(X)P$, output prefixing $\overline{a}\langle P\rangle P$, name restriction $\nu a.P$, and process replication $!P$. The output prefix construction illustrates the higher order aspect of the calculus, as a process (and not a name) is sent.

In process $a(X)P$, the variable X is bound. Similarly, in process $\nu a.P$, the name a is bound. We write $\mathrm{fv}(P)$ for the free variables of a process P, $\mathrm{fn}(P)$ for its free names, and $\mathrm{bn}(P)$ for its bound names. We write $P\{Q/X\}$ for the capture-free substitution of X by Q in P. For a name a and a process P, we write $a.P$ for $a(X)P$ where X is not free in P, and $\overline{a}.P$ for $\overline{a}\langle\mathbf{0}\rangle P$.

Remark 1. *As in many other higher order calculi, replication does not have to be built in as it can be encoded using the other constructs. To encode replication in HOπ without replication, we first define Y as $t(X)(P \mid X \mid \overline{t}\langle X\rangle\mathbf{0})$. We then encode $!P$ by the process $Q = \nu t.(\overline{t}\langle Y\rangle\mathbf{0} \mid Y)$. The process Y is similar to a copy of P, except that it receives a copy of itself on t in order to launch a copy of P and recreate the process Q. Hence the process Q reduces to $P \mid Q$, like the process $!P$.*

To encode replication of prefixed processes $!m.P$, we instead define Y as $m.t(X)(P \mid X \mid \overline{t}\langle X\rangle\mathbf{0})$. We then encode $!m.P$ by the process $Q = \nu t.(\overline{t}\langle Y\rangle\mathbf{0} \mid Y)$.

These encodings introduce an extra step to unfold the replication, which raises issues with strong behavioral equivalences. We thus keep replication explicitly in the calculus.

Convention. We identify processes up to α-conversion of names and variables: processes and agents are always chosen such that their bound names and variables are distinct from free names and variables. In any discussion or proof,

$$P \mid (Q \mid R) \equiv (P \mid Q) \mid R \qquad P \mid Q \equiv Q \mid P \qquad P \mid \mathbf{0} \equiv P$$

$$\nu a.\nu b.P \equiv \nu b.\nu a.P \qquad \nu a.\mathbf{0} \equiv \mathbf{0} \qquad \nu a.(P \mid Q) \equiv P \mid \nu a.Q \qquad !P \equiv P \mid !P$$

$$a(X)P \xrightarrow{a} (X)P \ \textsc{Abstr} \qquad \overline{a}\langle Q\rangle P \xrightarrow{\overline{a}} \langle Q\rangle P \ \textsc{Concr}$$

$$\frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} \ \textsc{Par} \qquad \frac{P \xrightarrow{\alpha} A}{\nu a.P \xrightarrow{\alpha} \nu a.A} \ \textsc{Restr} \qquad \frac{P \xrightarrow{\alpha} A}{!P \xrightarrow{\alpha} A \mid !P} \ \textsc{Replic}$$

$$\frac{P \xrightarrow{a} F \qquad P \xrightarrow{\overline{a}} C}{!P \xrightarrow{\tau} F \bullet C \mid !P} \ \textsc{Replic-HO} \qquad \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \ \text{HO}$$

Figure 2: Structural Congruence and Contextual Labeled Transition System for HOπ

we assume that bound names and bound variables of any process or actions under consideration are chosen to be different from the names and variables occurring free in any other entities under consideration. Note that with this convention, we have $\nu a.(P \mid Q) \equiv P \mid \nu a.Q$ in Figure 2, without qualification on the free names of P. For the same reason, we do not have any side condition in the rule Restr: because a is bound in $\nu a.P$, it cannot be free in the action α.

We now recall structural congruence and the rules of the labelled transition system in Figure 2, omitting the symmetric rules for Par and HO. Because of the convention on bound and free names, we do not need a side-condition in rule Restr. A process may evolve towards a process (internal actions $P \xrightarrow{\tau} P'$), an *abstraction* (message input $P \xrightarrow{a} F = (X)Q$), or a *concretion* (message output $P \xrightarrow{\overline{a}} C = \nu\widetilde{b}.\langle R\rangle Q$). The transition $P \xrightarrow{a} (X)Q$ means that P may receive a process R on a to continue as $Q\{R/X\}$. The transition $P \xrightarrow{\overline{a}} \nu\widetilde{b}.\langle R\rangle Q$ means that P may send the process R on a and continue as Q, and that the scope of names $\widetilde{b}$, which occur free in R, has to be expanded to encompass the recipient of R.

A synchronous higher-order communication takes place when a concretion interacts with an abstraction (rule HO). We define a pseudo-application operator $\bullet$ between an abstraction $F = (X)P$ and a concretion $C = \nu\widetilde{b}.\langle R\rangle Q$ as follows.

$$(X)P \bullet \nu\widetilde{b}.\langle R\rangle Q \triangleq \nu\widetilde{b}.(P\{R/X\} \mid Q)$$

As above, we rely on the convention on bound and free names to avoid name capture. We write $(X)P \circ Q$ for the application of the abstraction $(X)P$ to the process Q, and define it as follows.

$$(X)P \circ Q \triangleq P\{Q/X\}$$

Let *agents*, noted A, be the set of processes, abstractions, and concretions.

We extend the parallel composition and restriction operators to all agents as follows.

$$
\begin{array}{ll}
(X)Q \mid P \triangleq (X)(Q \mid P) & \nu\widetilde{b}.\langle Q\rangle R \mid P \triangleq \nu\widetilde{b}.\langle Q\rangle(R \mid P) \\
P \mid (X)Q \triangleq (X)(P \mid Q) & P \mid \nu\widetilde{b}.\langle Q\rangle R \triangleq \nu\widetilde{b}.\langle Q\rangle(P \mid R) \\
\nu a.(X)Q \triangleq (X)\nu a.P & \nu a.\nu\widetilde{b}.\langle Q\rangle R \triangleq \nu\widetilde{b}, a.\langle Q\rangle R \quad \text{if } a \in \mathrm{fn}(Q) \\
 & \nu a.\nu\widetilde{b}.\langle Q\rangle R \triangleq \nu\widetilde{b}.\langle Q\rangle \nu a.R \quad \text{if } a \notin \mathrm{fn}(Q)
\end{array}
$$

Barbed congruence is the classic reduction-based behavioral equivalence. We define reduction $\longrightarrow$ as $\equiv\stackrel{\tau}{\longrightarrow}\equiv$ and weak reduction $\Longrightarrow$ as the reflexive and transitive closure of $\longrightarrow$. Observables γ of a process P, written $P\downarrow_\gamma$, are unrestricted names or conames on which a communication may immediately occur. Contexts $\mathbb{C}$ are terms with a hole $\Box$. Filling the hole with a process P is written $\mathbb{C}\{P\}$; the capture of some free names of P may happen during the operation. In a context, we cannot perform α-conversion on names that are bound at the hole position. For example, the name a cannot be α-converted in $\nu a.(\Box \mid P)$, but can be α-converted in $\Box \mid (\nu a.P)$. In $\mathbb{C} = \nu a.((\nu a.\Box) \mid a.\mathbf{0})$, the outermost restriction on a cannot bind a free name at the hole position; therefore, $\mathbb{C}$ can be α-converted into $\nu b.((\nu a.\Box) \mid b.\mathbf{0})$. A relation $\mathcal{R}$ is a *congruence* iff $P\ \mathcal{R}\ Q$ implies $\mathbb{C}\{P\}\ \mathcal{R}\ \mathbb{C}\{Q\}$ for all $\mathbb{C}$.

Definition 1. *A symmetric relation on closed processes $\mathcal{R}$ is a strong barbed bisimulation iff $P\ \mathcal{R}\ Q$ implies:*

- *for all $P\downarrow_\gamma$, we have $Q\downarrow_\gamma$;*
- *for all $P \longrightarrow P'$, there exists Q' such that $Q \longrightarrow Q'$ and $P'\ \mathcal{R}\ Q'$.*

Two processes P, Q are strong barbed congruent*, written $P \sim_b Q$, if for all $\mathbb{C}$ there exists a strong barbed bisimulation $\mathcal{R}$ such that $\mathbb{C}\{P\}\ \mathcal{R}\ \mathbb{C}\{Q\}$.*

Definition 2. *A symmetric relation on closed processes $\mathcal{R}$ is a weak barbed bisimulation iff $P\ \mathcal{R}\ Q$ implies:*

- *for all $P\downarrow_\gamma$, we have $Q \Longrightarrow\downarrow_\gamma$;*
- *for all $P \longrightarrow P'$, there exists Q' such that $Q \Longrightarrow Q'$ and $P'\ \mathcal{R}\ Q'$.*

Two processes P, Q are weak barbed congruent*, written $P \approx_b Q$, if for all $\mathbb{C}$ there exists a weak barbed bisimulation $\mathcal{R}$ such that $\mathbb{C}\{P\}\ \mathcal{R}\ \mathbb{C}\{Q\}$.*

A relation $\mathcal{R}$ is *sound* with respect to another relation $\mathcal{R}'$ iff $\mathcal{R}\subseteq\mathcal{R}'$; $\mathcal{R}$ is *complete* with respect to $\mathcal{R}'$ iff $\mathcal{R}'\subseteq\mathcal{R}$. If $\mathcal{R}$ is both sound and complete with respect to $\mathcal{R}'$, then it *characterizes* $\mathcal{R}'$. In the following, we will be interested in relations that are at least sound with respect to strong or weak barbed congruence, and in relations that characterize them.

In [37], Sangiorgi proposed *context* bisimilarities as alternatives to barbed congruence.

Definition 3. *Early strong context bisimilarity $\sim$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}\ Q'$;*
- *for all $P \xrightarrow{a} F$, for all C, there exists F' such that $Q \xrightarrow{a} F'$ and $(F \bullet C)\ \mathcal{R}\ (F' \bullet C)$;*
- *for all $P \xrightarrow{\overline{a}} C$, for all F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $(F \bullet C)\ \mathcal{R}\ (F \bullet C')$.*

Note. The late variant of strong context bisimulation can simply be obtained by changing the order of quantifications on concretions and abstractions in the above clauses. Thus the clause for input in late style would be:
for all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and for all C, we have $(F \bullet C)\ \mathcal{R}\ (F' \bullet C)$.

As shown by Sangiorgi [36, 37], strong early context bisimilarity characterizes strong barbed congruence:

Theorem 1. *We have $\sim\ = \sim_b$.*

Let us turn now to the weak case. We write $\stackrel{\tau}{\Rightarrow}$ for the reflexive and transitive closure of $\xrightarrow{\tau}$. For every name or coname γ, we write $\stackrel{\gamma}{\Rightarrow}$ for $\stackrel{\tau}{\Rightarrow}\xrightarrow{\gamma}$. As higher order steps result in concretions and abstractions, they may not reduce further; silent steps after this reduction are taken into account in the definition of weak simulation. We define early weak context bisimilarity as:

Definition 4. *Early weak context bisimilarity $\approx$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$;*
- *for all $P \xrightarrow{a} F$, for all C, there exist F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \bullet C \stackrel{\tau}{\Rightarrow} Q'$, and $F \bullet C\ \mathcal{R}\ Q'$;*
- *For all $P \xrightarrow{\overline{a}} C$, for all F, there exist C', Q' such that $Q \stackrel{\overline{a}}{\Rightarrow} C'$, $F \bullet C' \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet C\ \mathcal{R}\ Q'$.*

Sangiorgi proves the soundness of $\approx$ in [37]:

Theorem 2. *We have $\approx\ \subseteq\ \approx_b$.*

Using the same technique as in the π-calculus [39], one can prove that $\approx$ is also complete on *image-finite* processes.

Definition 5. *A process P is image finite iff*

- *the set $\{P' \mid P \stackrel{\tau}{\Rightarrow} P'\}$ is finite;*
- *for all a, C, the set $\{P' \mid \exists F, P \stackrel{a}{\Rightarrow} F \wedge (F \bullet C) \stackrel{\tau}{\Rightarrow} P'\}$ is finite;*
- *for all a, F, the set $\{P' \mid \exists C, P \stackrel{\overline{a}}{\Rightarrow} C \wedge (F \bullet C) \stackrel{\tau}{\Rightarrow} P'\}$ is finite.*

Theorem 3. *We have $\approx_b \subseteq \approx$ on image-finite processes.*

Context bisimulation may be understood as follows: when two tested processes P and Q perform a partial action, such as sending or receiving a message, the bisimulation considers every context which may complement the action. It is easier to manipulate than barbed congruence, since it features only one test in the internal action case. However, the universal quantification on concretions or abstractions makes the definition still unpractical to use. To address this issue, a simpler behavioral equivalence for HOπ, called *normal bisimulation*, was invented by Sangiorgi.

2.2. Normal bisimulation

Normal bisimulation is a behavioral equivalence that reduces the number of tests for each pair of processes under consideration. It relies on an encoding of HOπ in a first-order π-calculus, leveraging the limited uses of a received process: whether to duplicate or discard it, and when to run or forward the copies. These behaviors can be simulated by replacing the process P by a name which is used as a trigger to create a copy of P when needed. Formally, we have the following *factorization* theorem:

Theorem 4. *For every agent A, process Q, and name m with $m \notin fn(A, Q)$, the agents $A\{Q/X\}$ and $\nu m.(A\{\overline{m}.\mathbf{0}/X\} \mid !m.Q)$ are weakly late context bisimilar.*

The factorization theorem replaces a process Q by a trigger $\overline{m}.\mathbf{0}$ that may activate a copy of Q on demand. This copy is provided by the associated process $!m.Q$. Normal bisimulation relies on this translation to test equivalences of processes.

Definition 6. *Normal bisimilarity is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$;*
- *for all $P \xrightarrow{a} F$, there exist F', Q' and a fresh name m such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ \overline{m}.\mathbf{0} \stackrel{\tau}{\Rightarrow} Q'$ and $F \circ \overline{m}.\mathbf{0}\ \mathcal{R}\ Q'$;*
- *for all $P \xrightarrow{\overline{a}} \nu\widetilde{b}.\langle R\rangle S$, there exist a concretion $\nu\widetilde{b'}.\langle R'\rangle S'$, a process Q', and a fresh name m such that $Q \stackrel{\overline{a}}{\Rightarrow} \nu\widetilde{b'}.\langle R'\rangle S'$, $\nu\widetilde{b'}.(S' \mid !m.R') \stackrel{\tau}{\Rightarrow} Q'$, and $\nu\widetilde{b}.(S \mid !m.R)\ \mathcal{R}\ Q'$.*

In the message input case, normal bisimilarity tests only a fresh trigger. In the message sending case, normal bisimilarity tests processes where the emitted processes R and R' are made available through a name m. Using the factorization theorem and the fact that weak late context bisimulation is a congruence, Sangiorgi proved that normal bisimilarity coincides with weak late context bisimilarity. Cao [6] extended the result to the strong case.

To summarize, context bisimulation is a first step in finding a simple behavioral equivalence: it reduces only slightly the quantifications. Normal bisimulation goes much further as only one test is performed for each transition step of a process pair. We now study such relations for more expressive calculi.

2.3. Syntax and semantics of HOπP

We now study bisimulations in calculi with passivation capabilities as in Homer or Kell. Instead of working in Homer or Kell directly, we define a simpler calculus called HOπ with Passivation (HOπP), which extends HOπ with a passivation operator. By doing this we avoid the unnecessary (for this study) features of Homer and Kell (mainly additional control on communication), and we are able to compare more directly bisimulations in HOπ and HOπP.

We add localities $a[P]$, that are passivation units, to the HOπ constructs. With the same notations as for HOπ, the syntax of HOπP is as follows.

$$P ::= \mathbf{0} \;\mid\; X \;\mid\; P \mid P \;\mid\; a(X)P \;\mid\; \overline{a}\langle P\rangle P \;\mid\; \nu a.P \;\mid\; !P \;\mid\; a[P]$$

When passivation is not triggered, a locality $a[P]$ is a transparent evaluation context: process P may evolve by itself and communicate freely with processes outside of locality a. At any time, passivation may be triggered and the process $a[P]$ becomes a concretion $\langle P\rangle\mathbf{0}$. Passivation may thus occur as an internal τ step only if there is a receiver on a ready to receive the contents of the locality.

We extend localities to all agents: if $F = (X)P$, then $a[F] \stackrel{\Delta}{=} (X)a[P]$; if $C = \nu\widetilde{b}.\langle Q\rangle R$, then $a[C] \stackrel{\Delta}{=} \nu\widetilde{b}.\langle Q\rangle a[R]$. We also add the following rules to the labeled transition system.

$$\frac{P \stackrel{\alpha}{\rightarrow} A}{a[P] \stackrel{\alpha}{\rightarrow} a[A]}\ \textsc{Loc} \qquad\qquad a[P] \stackrel{\overline{a}}{\rightarrow} \langle P\rangle\mathbf{0}\ \textsc{Passiv}$$

Note that rule Loc implies that the scope of restricted names may cross locality boundaries. Scope extrusion outside localities is performed "by need" when a communication takes place. Structural congruence follows the same rules as in HOπ (Figure 2), and as a consequence does not allow the restriction and locality operators to commute freely. If it did, structurally congruent processes would not be contextually bisimilar. For instance, let $Q = a[\nu b.P] \mid a(X)(X \mid X)$. It reduces to $(\nu b.P) \mid (\nu b.P)$ by triggering the passivation. If we allow the structural extrusion of νb across locality a, we would have $Q \equiv \nu b.(a[P] \mid a(X)(X \mid X))$, which evolves to $\nu b.(P \mid P)$. In this case, the name b is shared by the two instances of P, whereas each instance of P has its own name b in the first case. The two obtained processes may have different reductions. For example, assume that $P = \overline{b}.\mathbf{0} \mid b.b.R$.

- In the first case, we have $(\nu b.(\overline{b}.\mathbf{0} \mid b.b.R)) \mid (\nu b.(\overline{b}.\mathbf{0} \mid b.b.R))$, which evolves to $(\nu b.b.R) \mid (\nu b.b.R)$. No further reduction is possible.
- In the second case, we get $\nu b.(\overline{b}.\mathbf{0} \mid \overline{b}.\mathbf{0} \mid b.b.R \mid b.b.R)$, which may evolve to $\nu b.(R \mid b.b.R)$. All the reductions of R are possible.

2.4. Context bisimilarity

As in HOπ, our goal is to find a simple bisimulation-based characterization of barbed congruence. Observables for HOπP are unrestricted names or conames on which a communication or a passivation may immediately occur. The definition of strong barbed congruence is identical to Definition 1.

We now define a sound and complete context bisimulation for HOπP in the strong case. We first notice that the context bisimulation given by Sangiorgi for HOπ (Definition 3) is not sound in our calculus because of passivation. For example, the HOπ bisimilarity relates the following processes.

$$P_0 = \overline{a}\langle \mathbf{0} \rangle !m.\mathbf{0} \qquad Q_0 = \overline{a}\langle m.\mathbf{0} \rangle !m.\mathbf{0}$$

The differences between the emitted processes $\mathbf{0}$ and $m.\mathbf{0}$ are shadowed by the process $!m.\mathbf{0}$. More precisely, we have to check that for all F, the processes $(F \bullet \langle \mathbf{0} \rangle !m.\mathbf{0})$ and $(F \bullet \langle m.\mathbf{0} \rangle !m.\mathbf{0})$ are context bisimilar, i.e., for all R, we have $P' \triangleq R\{\mathbf{0}/X\} \mid !m.\mathbf{0}$ in relation with $Q' \triangleq R\{m.\mathbf{0}/X\} \mid !m.\mathbf{0}$. We have three kinds of possible transitions from P':

- transitions from R alone: they are matched by the same transitions of R in Q';
- synchronizations between $!m.\mathbf{0}$ and R or $\xrightarrow{m}$-transitions from $!m.\mathbf{0}$: they are matched by the same transitions in Q';
- synchronizations between the copies of the message $m.\mathbf{0}$ and R or $\xrightarrow{m}$-transitions from the message: they are matched by synchronizations between $!m.\mathbf{0}$ and R or $\xrightarrow{m}$-transitions from $!m.\mathbf{0}$ in Q'.

Conversely the transitions of Q' are matched by P'.

Remark 2. *This result can be proven formally by considering the symmetric closure of relation* $\{(P\{m.\mathbf{0}/X\} \mid !m.\mathbf{0}, P\{\mathbf{0}/X\} \mid !m.\mathbf{0})\}$*, and showing that this relation is an early strong bisimulation according to definition 3.*

However P_0 and Q_0 are not barbed congruent in HOπP. The context $\mathbb{C} = b[\Box] \mid a(X)X \mid b(X)\mathbf{0}$ distinguishes them. We have $\mathbb{C}\{P_0\} \longrightarrow b[!m.\mathbf{0}] \mid \mathbf{0} \mid b(X)\mathbf{0} = P'$ by a communication on a. This reduction is matched by $\mathbb{C}\{Q_0\} \longrightarrow b[!m.\mathbf{0}] \mid m.\mathbf{0} \mid b(X)\mathbf{0} = Q'$. By triggering the passivation on b, we have $P' \longrightarrow \mathbf{0}$ and $Q' \longrightarrow m.\mathbf{0}$. The two resulting processes are not barbed bisimilar.

In a concretion $\nu\widetilde{a}.\langle R \rangle S$, the emitted process R may be sent outside a locality b while the continuation S stays in b. If the passivation on b is triggered, S may be destroyed (as with P_0 and Q_0) or put in a different context. Hence the passivation may separate the processes R and S and put them in totally different contexts, which is not possible in a calculus without passivation. As in Kell and Homer, we address this issue by testing messages and continuations in different *evaluation contexts* $\mathbb{E}$. These contexts, when applied to concretions,

take into account the fact that a message and its continuation are separated: in the definition of $a[C]$ for some concretion C, the message part of C is put outside the locality whereas the continuation part remains inside. The grammar of HOπP evaluation contexts is:

$$\mathbb{E} ::= \Box \mid \nu a.\mathbb{E} \mid \mathbb{E} \mid P \mid P \mid \mathbb{E} \mid a[\mathbb{E}]$$

We call these contexts used for observational purposes *bisimulation contexts*. Early strong context bisimulation for HOπP is defined as follows.

Definition 7. *Early strong context bisimilarity $\sim$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P \mathcal{R} Q$ implies $fn(P) = fn(Q)$ and:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathcal{R} Q'$;*
- *for all $P \xrightarrow{a} F$, for all C, there exists F' such that $Q \xrightarrow{a} F'$ and $(F \bullet C) \mathcal{R} (F' \bullet C)$;*
- *for all $P \xrightarrow{\overline{a}} C$, for all F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}$, we have $(F \bullet \mathbb{E}\{C\}) \mathcal{R} (F \bullet \mathbb{E}\{C'\})$.*

This definition is similar to the ones for context bisimilarities in Homer [17] and Kell [41] (except that in Kell, contexts are also added in the abstraction case). The condition $\mathrm{fn}(P) = \mathrm{fn}(Q)$ has been added because of lazy scope extrusion: two bisimilar processes with different free names may be distinguished. For instance, a process P which cannot perform any transition but with a free name b (e.g. $\nu a.a.b.\mathbf{0}$) may be distinguished from $\mathbf{0}$ by a context $\mathbb{C} = c[\nu b.\overline{d}\langle\Box\rangle R] \mid d(X)c(Y)(Y \mid Y)$. The process $\mathbb{C}\{P\}$ may reduce to $\nu b.(R \mid R)$, whereas the process $\mathbb{C}\{\mathbf{0}\}$ evolves toward $(\nu b.R) \mid (\nu b.R)$. With an appropriate R, the two processes have different transitions, as illustrated in Section 2.3.

Example 1. *The tests within contexts $\mathbb{E}$ make the HOπP context bisimilarity $\sim$ more discriminant than the HOπ one. However, the relation $\sim$ is still bigger than trivial equivalences, such as structural congruence $\equiv$. For instance, the processes $m.\mathbf{0} \mid !a[m.\mathbf{0}] \mid !a[\mathbf{0}]$ and $!a[m.\mathbf{0}] \mid !a[\mathbf{0}]$ are early context bisimilar but not structural congruent.*

Remark 3. *In the concretion case, one could imagine tests with localities $F \bullet b[C]$, for a fresh name b, instead of tests with bisimulation contexts $F \bullet \mathbb{E}\{C\}$. The two tests are almost equivalent, except that tests with contexts $\mathbb{E}$ allow capture of free names of C. More precisely, let $C = \nu\widetilde{a}.\langle R\rangle S$; by passivation of b, we have $(F \bullet b[C]) \mid b(X)Q \xrightarrow{\tau} \nu\widetilde{a}.((F \circ R) \mid Q\{S/X\})$. Unlike in $\mathbb{E}\{S\}$, free names of S cannot be captured in $Q\{S/X\}$. Contexts $\mathbb{E}$ may also capture free names of the message R. Allowing capture makes proofs on $\sim$ easier; we conjecture that testing using capture-free evaluation contexts is enough for soundness.*

The definition of context bisimilarity is similar in the weak case.

Definition 8. *Early weak context bisimilarity $\approx$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$;*
- *for all $P \xrightarrow{a} F$, for all C, there exist F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $(F' \bullet C) \stackrel{\tau}{\Rightarrow} Q'$, and $(F \bullet C)\ \mathcal{R}\ Q'$;*
- *For all $P \xrightarrow{\overline{a}} C$, for all F, there exists C' such that $Q \stackrel{\overline{a}}{\Rightarrow} C'$ and for all $\mathbb{E}$, there exists Q' such that $(F \bullet \mathbb{E}\{C'\}) \stackrel{\tau}{\Rightarrow} Q'$ and $(F \bullet \mathbb{E}\{C\})\ \mathcal{R}\ Q'$.*

In the following section, we discuss techniques developed for Kell and for Homer that can be used to show that context bisimulation is sound and complete in the strong case. We also explain why these techniques fail in the weak case with early context bisimilarity.

3. Congruence proofs

3.1. Kell soundness proof

As in HOπ, the soundness proof used for Kell relies on a substitution lemma.

Lemma 1. *Let A be an agent and P, Q be processes; if P and Q are strong (respectively weak) context bisimilar, then $A\{P/X\}$ and $A\{Q/X\}$ are strong (respectively weak) context bisimilar.*

The approach of [37] to prove this lemma in HOπ can be summed up by:

- the result is proved for evaluation contexts (parallel composition, replication, and restriction);
- the result is proved for all processes, using the first step.

The distinction is useful since if A is an evaluation context, the reductions of $A\{P/X\}$ may come from A or P, whereas if A is not an evaluation context, P cannot be reduced. However, this method fails with HOπP. Unlike HOπ, an execution context in HOπP may become a non-execution context (a locality may become a message output preventing internal reductions).

More precisely, to show the first step of Sangiorgi's method in the locality case, we would have to prove that if $P \sim Q$, then $a[P] \sim a[Q]$. We would thus have to build a relation $\mathcal{R}$ such that (assuming $P \sim Q$):

$$\begin{array}{ccc} a[P] & \stackrel{\mathcal{R}}{\text{———}} & a[Q] \\ \Big\downarrow{\scriptstyle \overline{a}} & & \Big\downarrow{\scriptstyle \overline{a}} \\ \langle P\rangle\mathbf{0} & \stackrel{\mathcal{R}}{\text{– –}} & \langle Q\rangle\mathbf{0} \end{array}$$

and such that $\mathcal{R}$ is a bisimulation[5]. Therefore for all abstractions $(X)R$, we would have $R\{P/X\}\ \mathcal{R}\ R\{Q/X\}$. To prove a sub-case of the substitution lemma, we would have to consider the relation $\mathcal{R} = \{(R\{P/X\}, R\{Q/X\}), P \sim Q\}$ and show that it is a bisimulation. But this would be the same as proving the substitution lemma directly, making the approach fail.

The method used for the Kell-calculus is the following one. For two finite sets of processes $\widetilde{P} = (P_i)_{i\in\mathcal{I}}$, $\widetilde{Q} = (Q_i)_{i\in\mathcal{I}}$ of the same size and a relation $\mathcal{R}$, we write $\widetilde{P}\ \mathcal{R}\ \widetilde{Q}$ iff we have $P_i\ \mathcal{R}\ Q_i$ for all $i \in \mathcal{I}$. We define a relation

$$\mathcal{R} = \{(\mathbb{C}\{R\{\widetilde{P}/\widetilde{Y}\}\}, \mathbb{C}\{R\{\widetilde{Q}/\widetilde{Y}\}\}), \mathrm{fv}(R) = \widetilde{Y}, \widetilde{P} \sim \widetilde{Q}\}$$

and we show that its reflexive and transitive closure is a bisimulation. We assume now that we work with the early definition, but the proof technique works with the late one as well. The candidate relation requires contexts $\mathbb{C}$ in its definition to take into account name capture, which may happen in the message output tests because of bisimulation contexts $\mathbb{E}$.

We first explain why we work with the reflexive and transitive closure instead of the relation itself. To show that $\mathcal{R}$ is a bisimulation, we proceed by structural induction on $\mathbb{C}$, and we perform a nested induction on the derivation of the transition $\mathbb{C}\{R\{\widetilde{P}/\widetilde{Y}\}\} \xrightarrow{\alpha} R'$. For any agent A and processes $\widetilde{P}$, we write $A_{\widetilde{P}}$ for $A\{\widetilde{P}/\widetilde{Y}\}$. Suppose $\mathbb{C} = \Box$ and consider the case where $R = R^1 \mid R^2$, and R evolves by a higher-order communication. We want to close the following diagram

$$\begin{array}{ccc} R^1_{\widetilde{P}} \mid R^2_{\widetilde{P}} & \overset{\mathcal{R}}{\text{———}} & R^1_{\widetilde{Q}} \mid R^2_{\widetilde{Q}} \\ \Big\downarrow \tau & & \\ F_{\widetilde{P'}} \bullet C_{\widetilde{P''}} & & \end{array}$$

knowing that $R^1_{\widetilde{P}} \xrightarrow{a} F_{\widetilde{P'}}$ and $R^2_{\widetilde{P}} \xrightarrow{\overline{a}} C_{\widetilde{P''}}$ for some a. By definition we have $R^1_{\widetilde{P}}\ \mathcal{R}\ R^1_{\widetilde{Q}}$ so by applying $C_{\widetilde{P''}}$ to $F_{\widetilde{P'}}$ (we work with early bisimulation, hence we have to choose the concretion before getting a matching abstraction), we have by induction:

$$\begin{array}{ccc} R^1_{\widetilde{P}} & \overset{\mathcal{R}}{\text{———}} & R^1_{\widetilde{Q}} \\ \Big\downarrow a & & \Big\vdots\, a \\ F_{\widetilde{P'}} & \overset{\mathcal{R}}{\text{- - -}} & F_{\widetilde{Q'}} \end{array}$$

[5]Note that $\mathcal{R}$ relates processes only, but we use $\mathcal{R}$ to relate agents in some diagrams for simplicity

with $F_{\widetilde{P'}} \bullet C_{\widetilde{P''}} \mathcal{R} F_{\widetilde{Q'}} \bullet C_{\widetilde{P''}}$.

We have $R^2_{\widetilde{P}} \mathcal{R} R^2_{\widetilde{Q}}$, so by applying $C_{\widetilde{P''}}$ to $F_{\widetilde{Q'}}$ we have:

$$\begin{array}{ccc} R^2_{\widetilde{P}} & \overset{\mathcal{R}}{\text{———}} & R^2_{\widetilde{Q}} \\ \Big\downarrow{\scriptstyle \overline{a}} & & \Big\downarrow{\scriptstyle \overline{a}} \\ C_{\widetilde{P''}} & \overset{\mathcal{R}}{\text{– –}} & C_{\widetilde{Q''}} \end{array}$$

with $F_{\widetilde{Q'}} \bullet C_{\widetilde{P''}} \mathcal{R} F_{\widetilde{Q'}} \bullet C_{\widetilde{Q''}}$. From these we can conclude that:

$$\begin{array}{ccc} R^1_{\widetilde{P}} \mid R^2_{\widetilde{P}} & \overset{\mathcal{R}}{\text{———————}} & R^1_{\widetilde{Q}} \mid R^2_{\widetilde{Q}} \\ \Big\downarrow{\scriptstyle \tau} & & \Big\downarrow{\scriptstyle \tau} \\ F_{\widetilde{P'}} \bullet C_{\widetilde{P''}} & \overset{\mathcal{R}}{\text{– –}} & F_{\widetilde{Q'}} \bullet C_{\widetilde{P''}} \overset{\mathcal{R}}{\text{– –}} F_{\widetilde{Q'}} \bullet C_{\widetilde{Q''}} \end{array}$$

As a result, we have:

$$\begin{array}{ccc} R_{\widetilde{P}} & \overset{\mathcal{R}}{\text{———}} & R_{\widetilde{Q}} \\ \Big\downarrow{\scriptstyle \tau} & & \Big\downarrow \\ R'_{\widetilde{P'} \cup \widetilde{P''}} & \overset{\mathcal{R}^2}{\text{– –}} & R'_{\widetilde{Q'} \cup \widetilde{Q''}} \end{array}$$

while we need $R'_{\widetilde{P'} \cup \widetilde{P''}} \mathcal{R} R'_{\widetilde{Q'} \cup \widetilde{Q''}}$. More generally, we prove that $\mathcal{R}$ *progresses* towards its reflexive and transitive closure $\mathcal{R}^*$, in the sense of [39].

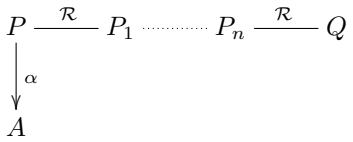
Definition 9. *Let $\mathcal{R}, \mathcal{S}$ two relations on processes. The relation $\mathcal{R}$ strongly progresses towards $\mathcal{S}$ in an early style iff $P \mathcal{R} Q$ implies $fn(P) = fn(Q)$ and:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathcal{S} Q'$;*
- *for all $P \xrightarrow{a} F$ and all C, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C \mathcal{S} F' \bullet C$;*
- *for all $P \xrightarrow{\overline{a}} F$ and all F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \mathcal{S} F \bullet \mathbb{E}\{C'\}$.*

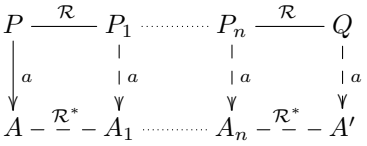
Using a diagram, we have:

$$\begin{array}{ccc} P & \overset{\mathcal{R}}{\text{———}} & Q \\ \Big\downarrow{\scriptstyle \alpha} & & \Big\downarrow{\scriptstyle \alpha} \\ A & \overset{\mathcal{R}^*}{\text{– –}} & A' \end{array}$$

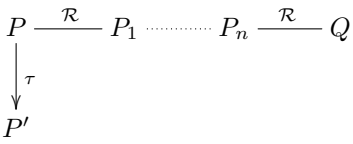
In the strong case, it is sufficient to show that $\mathcal{R}^*$ is a bisimulation. Suppose that $P \mathcal{R}^* Q$ and $P \xrightarrow{\alpha} A'$. There exists $P_1, \ldots, P_n$ such that $P \mathcal{R} P_1 \mathcal{R} \ldots P_n \mathcal{R} Q$. We want to close the following diagram:



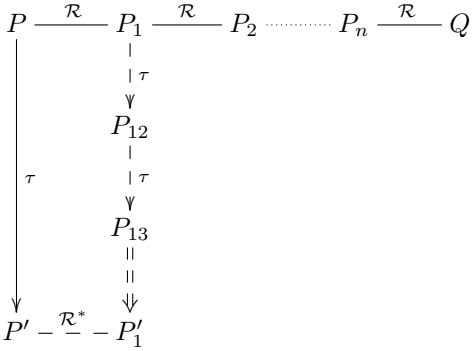
Since $\mathcal{R}$ progress towards $\mathcal{R}^*$, we build $A_1 \dots A_n, A'$ such that $A\ \mathcal{R}^*\ A_1\ \mathcal{R}^*\ \dots A_n\ \mathcal{R}^*\ A'$.



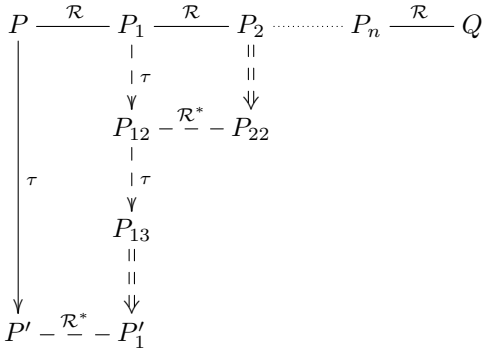
Since $\mathcal{R}^*$ is transitive, we have $A\ \mathcal{R}^*\ A'$ as required. The soundness proof using the Kell-calculus technique can be found in [24]. This approach fails in the weak case. Suppose now we have $P\ \mathcal{R}\ Q$ (where $\mathcal{R}$ is the congruence closure of the weak bisimilarity $\approx$) and $P \xrightarrow{\tau} P'$. We want to close the following diagram:



We use the fact that $\mathcal{R}$ progresses towards $\mathcal{R}^*$ for P, P', P_1. Suppose that, for instance, P_1 performs at least two internal actions.



We close the sub-diagram P_1, P_{12}, P_2:



Hence we have $P_{12}\ \mathcal{R}^*\ P_{22}$ and $P_{12} \xrightarrow{\tau} P_{13}$: the diagram P, Q, P' we want to close may be smaller than P_{12}, P_{22}, P_{13}. The scheme may then recursively and infinitely repeat itself. Knowing that $\mathcal{R}$ progress towards $\mathcal{R}^*$ does not allow to prove that $\mathcal{R}^*$ is a bisimulation in the weak case. This problem is similar to the application of up-to techniques in the weak case [31]. Hence we cannot show that the early bisimulation is a congruence in the weak case with this technique.

Remark 4. *We have the same results with the late bisimulation: we can prove that the late bisimulation is a congruence in the strong case, but not in the weak one.*

Remark 5. *On the contrary, the method used by Sangiorgi may easily be adapted in the weak case for HOπ without passivation. Transitivity issues are dealt with by using up-to techniques mixing strong and weak bisimilarities. See [37] for further details.*

3.2. Howe's Method

Howe's method [18, 1, 15] is a systematic proof technique to show that a simulation $\mathcal{R}$ is a congruence. The method can be divided in three steps: first, prove some basic properties on the *Howe's closure* $\mathcal{R}^\bullet$ of the relation. By construction, $\mathcal{R}^\bullet$ contains $\mathcal{R}$ and is a congruence. Second, prove a simulation-like property for $\mathcal{R}^\bullet$, and finally prove that $\mathcal{R}$ and $\mathcal{R}^\bullet$ coincide on closed processes. Since $\mathcal{R}^\bullet$ is a congruence, conclude that $\mathcal{R}$ is a congruence.

The definition of the Howe's closure relies on the open extension of $\mathcal{R}$, noted $\mathcal{R}^\circ$: it extends the definition of the relation $\mathcal{R}$ to *open processes*, that are processes with free process variables.

Definition 10. *Let P and Q be two open processes. We have $P\ \mathcal{R}^\circ\ Q$ iff $P\sigma\ \mathcal{R}\ Q\sigma$ for all process substitutions σ that close P and Q.*

Howe's closure is inductively defined as the smallest congruence which contains $\mathcal{R}^\circ$ and is closed under right composition with $\mathcal{R}^\circ$.

Definition 11. *Howe's closure $\mathcal{R}^\bullet$ of a relation $\mathcal{R}$ is the smallest relation verifying:*

- $\mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$;
- $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$;
- *for all operators op of the language, if* $\widetilde{P}\ \mathcal{R}^\bullet\ \widetilde{Q}$, *then* $op(\widetilde{P})\ \mathcal{R}^\bullet\ op(\widetilde{Q})$.

By definition, $\mathcal{R}^\bullet$ is a congruence, and the composition with $\mathcal{R}^\circ$ allows some transitivity and gives some additional properties to the relation.

Remark 6. *In the literature (e.g., [18, 15, 17]) Howe's closure is usually inductively defined by the following rule for all operators op in the language:*

$$\frac{\widetilde{P}\ \mathcal{R}^\bullet\ \widetilde{R} \qquad op(\widetilde{R})\ \mathcal{R}^\circ\ Q}{op(\widetilde{P})\ \mathcal{R}^\bullet\ Q}$$

Both definitions are equivalent (see [15] for the proof). We believe that Definition 11 is easier to understand and to work with in proofs.

In our case, we want to prove that a bisimilarity $\mathcal{B}$ is a congruence. By definition, we have $\mathcal{B}^\circ \subseteq \mathcal{B}^\bullet$. To have the reverse inclusion, we prove that $\mathcal{B}^\bullet$ is a bisimulation. To this end, we need the following classical properties of the Howe's closure.

Lemma 2. *Let* $\mathcal{R}$ *be a reflexive relation. If* $P\ \mathcal{R}^\bullet\ Q$ *and* $R\ \mathcal{R}^\bullet\ S$, *then we have* $P\{R/X\}\ \mathcal{R}^\bullet\ Q\{S/X\}$.

This lemma is typically used to establish the simulation-like result (second step of the method). We sketch the proof in order to give an idea on why the transitive item $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$ is needed in Definition 11. The proof is by induction on the derivation of $P\ \mathcal{R}^\bullet\ Q$. Suppose we have $P\ \mathcal{R}^\circ\ Q$. Since $R\ \mathcal{R}^\bullet\ S$ and $\mathcal{R}^\bullet$ is a congruence, we have $P\{R/X\}\ \mathcal{R}^\bullet\ P\{S/X\}$. Let σ be a substitution that closes P, Q, and S except for X; by open extension definition, we have $P\{S/X\}\sigma\ \mathcal{R}\ Q\{S/X\}\sigma$, i.e., we have $P\{S/X\}\ \mathcal{R}^\circ\ Q\{S/X\}$. Finally we have $P\{R/X\}\ \mathcal{R}^\bullet \mathcal{R}^\circ\ Q\{S/X\}$, hence we have $P\{R/X\}\ \mathcal{R}^\bullet\ Q\{S/X\}$. The other cases are easy using the induction hypothesis.

Remark 7. *One may define Howe's closure with* $\mathcal{R}^\circ \mathcal{R}^\bullet \subseteq \mathcal{R}^\bullet$ *as the transitive item instead of* $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$. *However left relation composition with* $\mathcal{R}^\circ$ *raises issues when proving weak simulation properties, while right relation composition works in the strong and weak cases.*

We cannot prove directly that $\mathcal{B}^\bullet$ is symmetric. Instead we use the following lemma.

Lemma 3. *Let* $\mathcal{R}$ *be an equivalence. Then the reflexive and transitive closure* $(\mathcal{R}^\bullet)^*$ *of* $\mathcal{R}^\bullet$ *is symmetric.*

Proof. By proving by induction that $P(\mathcal{R}^\bullet)^{-1}Q$ implies $P(\mathcal{R}^\bullet)^*Q$ for all P, Q. □

Then one proves that the restriction of $(\mathcal{B}^\bullet)^*$ to closed terms is a bisimulation, Consequently we have $\mathcal{B} \subseteq \mathcal{B}^\bullet \subseteq (\mathcal{B}^\bullet)^* \subseteq \mathcal{B}$ on closed terms, and we conclude that $\mathcal{B}$ is a congruence.

The main difficulty lies in the proof of the simulation-like property for Howe's closure. In the following subsection, we explain why we cannot directly use Howe's method with early context bisimilarity (Definitions 3 and 7).

3.3. Communication Problem

Proving that a congruence is a simulation raises transitivity issues, as we can see with the Kell proof method (Section 3.1). To avoid this problem, we establish a stronger result. Given a bisimilarity $\mathcal{B}$ based on a LTS $P \xrightarrow{\lambda} A$, the simulation-like result follows the pattern below, similar to a higher-order bisimilarity clause, such as the one for Plain CHOCS [43].

Let $P\ \mathcal{B}^\bullet\ Q$. If $P \xrightarrow{\lambda} A$, then for all $\lambda\ \mathcal{B}^\bullet\ \lambda'$, there exists B such that $Q \xrightarrow{\lambda'} B$ and $A\ \mathcal{B}^\bullet\ B$.

Early bisimulations are those where all the information about a step on one side is known before providing a matching step. In the higher-order setting with concretions and abstractions, it means that when an output occurs, the abstraction that will consume the output is specified before the matching step is given. In fact, the matching step may very well be different for a given output when the abstraction considered is different. Symmetrically, in the case of an input, the matching step is chosen depending on the input and the actual concretion that is provided. In both cases, this amounts to putting the abstraction in the label in the case of an output, and the concretion in the label in case of an input. One is thus lead to prove the following simulation property.

Conjecture 1. *If $P\ \mathcal{R}^\bullet\ Q$, then:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}^\bullet\ Q'$;*
- *for all $P \xrightarrow{a} F$, for all $C\ \mathcal{R}^\bullet\ C'$, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C\ \mathcal{R}^\bullet\ F' \bullet C'$;*
- *for all $P \xrightarrow{\overline{a}} C$, for all $F\ \mathcal{R}^\bullet\ F'$ there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\}\ \mathcal{R}^\bullet\ F' \bullet \mathbb{E}\{C'\}$.*

These clauses raise several issues. First, we have to find extensions of Howe's closure to abstractions and concretions which fit an early style. Even assuming such extensions, there are issues in the inductive proof of conjecture 1 with higher-order communication. The reasoning is by induction on $P\ \mathcal{R}^\bullet\ Q$. Suppose we are in the parallel case, i.e., we have $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$, with $P_1\ \mathcal{R}^\bullet\ Q_1$ and $P_2\ \mathcal{R}^\bullet\ Q_2$. Suppose that we have $P \xrightarrow{\tau} P'$, and the transition comes from rule HO: we have $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\overline{a}} C$ and $P' = F \bullet C$. We want to find Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}^\bullet\ Q'$. We also want to use the same rule HO, hence we have to find F', C' such that $Q \xrightarrow{\tau} F' \bullet C'$. However we

cannot use the input clause of the induction hypothesis with P_1, Q_1: to have a F' such that $Q_1 \xrightarrow{a} F'$, we have to find first a concretion C' such that $C \mathcal{R}^\bullet C'$. We cannot use the output clause with P_2, Q_2 either: to have a C' such that $Q_2 \xrightarrow{\overline{a}} C'$, we have to find first an abstraction F' such that $F \mathcal{R}^\bullet F'$. We cannot bypass this mutual dependency and the inductive proof of conjecture 1 fails.

Remark 8. *Note that the reasoning depends more on the bisimilarity than on the calculus: the same problem occurs with early context bisimilarities for HOπ, Homer, and the Kell calculus.*

A simple way to break the mutual dependency between concretions and abstractions is to give up on the early style. An approach, used in [14], is to change the output case to a late style (hence the name, *input-early*, of their bisimulation): an output is matched by another output *independently of the abstraction that receives it*. This breaks the symmetry and allows us to proceed forward: first find the matching output C', then for this C' find the matching input using the input-early relation $\sim_{ie}$. Howe's closure is then extended to concretions $C \sim_{ie}^\bullet C'$ and a simulation-like property similar to Conjecture 1 is shown, except that the output clause is changed into:

- for all $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $C \sim_{ie}^\bullet C'$.

However, in the weak case, this input-early approach does not result in a sound and complete characterization of weak barbed congruence. Definition of weak input-early bisimilarity has to be written in the *delay* style: internal actions are not allowed after a visible action. The delay style is necessary to keep the concretion clause independent from abstractions. It is not satisfactory since delay bisimilarities are generally not complete with respect to weak barbed congruence.

We thus propose a different approach, detailed in Section 4, that works with weak bisimulations defined in the early non-delay style. In our solution, the output clause is not late, just a little less early. More precisely, instead of requiring the abstraction before providing a matching output, we only require the process that will do the reception (that will reduce to the abstraction). This may seem a very small change, yet it is sufficient to break the symmetry. We return to the communication problem where $P_1 \mid P_2$ is in relation with $Q_1 \mid Q_2$. The concretion C' from Q_2 matching the $P_2 \xrightarrow{\overline{a}} C$ step depends only on Q_1, which is known, and not on some unknown abstraction. We can then obtain the abstraction F' from Q_1 that matches the $P_1 \xrightarrow{a} F$ step. This abstraction depends fully on C', in the usual early style. Technically, we do not use concretions and abstractions anymore. In the LTS, when a communication between P and Q occurs, this becomes a transition from P using Q as a label (rule HO^p_τ in Fig. 4). Higher in the derivation, the actual output from P is discovered, and we switch to dealing with the input knowing exactly the output (rule $\textsc{Out}^p_o$ in Fig. 5). The proof of the bisimulation property for the candidate relation relies on this serialization of the LTS, which illustrates the break in the

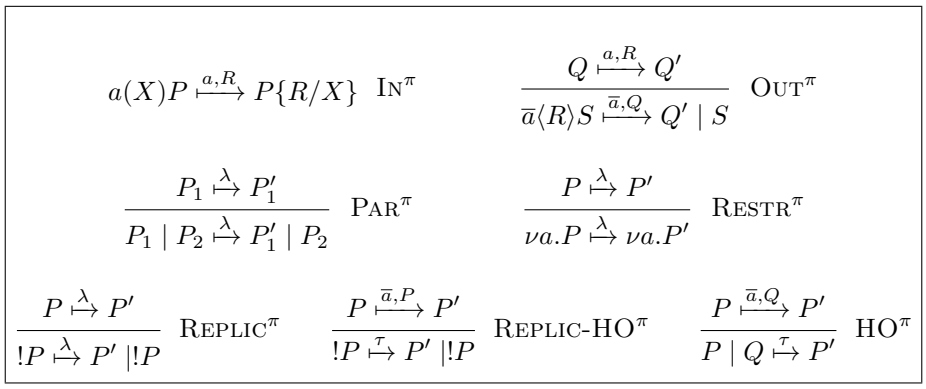


Figure 3: Complementary LTS for HOπ

symmetry. On the other hand, the gap between a completely early relation and this one is small enough to let us prove that they actually coincide.

4. Complementary semantics for HOπ

We now propose a new semantics for HOπ that coincide with the contextual one yet allow the use of Howe's method to prove soundness of early bisimilarities.

4.1. Complementary LTS

We define a LTS $P \overset{\lambda}{\mapsto} P'$ where processes always evolve towards other processes. We have three kinds of transitions: internal actions $P \overset{\tau}{\mapsto} P'$, message input $P \overset{a,R}{\longmapsto} P'$, and message output $P \overset{\overline{a},R}{\longmapsto} P'$. We call this new LTS *complementary* since in the output action, we put the context which complements P in the label λ of the transition. Rules of the LTS can be found in Figure 3, except for the symmetric of rules PAR$^\pi$ and HO$^\pi$.

Rules for internal actions $P \overset{\tau}{\mapsto} P'$ are similar to the one for the contextual LTS $P \overset{\tau}{\to} P'$, except for higher-order communication since we change the message output judgement; we detail rule HO$^\pi$ later. Message input $P \overset{a,R}{\longmapsto} P'$ means that process P may receive the process R as a message on a and becomes P'. In the contextual style, it means that $P \overset{a}{\to} F$ and $P' = F \circ R$ for some F; complementary message input is just a contextual message input written in the early style.

The main difference is in how we define output actions. The transition $P \overset{\overline{a},R}{\longmapsto} P'$ means that P may send a message on a, R may receive on a, and the communication on a between P and R results in P'. It is not the same as writing contextual transition $P \overset{\overline{a}}{\to} C$ in an early style; instead of putting an abstraction F in the label, we put a process R. The transition $P \overset{\overline{a},R}{\longmapsto} P'$ means that there exists F, C such that $P \overset{\overline{a}}{\to} C$, $R \overset{a}{\to} F$, and $P' = F \bullet C$.

Rules of the LTS (Figure 3) are classic except rules HO^π and OUT^π. With our convention on bound and free names, we do not have a side-condition in rule RESTR^π: because a is bound in $\nu a.P$, it cannot be free in λ, so if $\lambda = b, R$ or $\lambda = \overline{b}, R$, then we have $a \neq b$ and $a \notin \text{fn}(R)$. In rule HO^π, the premise $P \overset{\overline{a},Q}{\longmapsto} P'$ means that P and Q can communicate on a name a and the result is P', i.e., $P \mid Q \xrightarrow{\tau} P'$ (by communication on a), which is exactly what the conclusion of the rule states. Rule OUT^π has a premise (unlike its equivalent rule CONCR) since in the conclusion we need the result Q' of the input of R on a by Q.

The complementary LTS has the same semantics as the contextual LTS, as stated in the following lemma:

Lemma 4. *Let P be an HOπ process.*

- *We have $P \xrightarrow{\tau} \equiv P'$ iff $P \overset{\tau}{\longmapsto} \equiv P'$.*
- *If $P \xrightarrow{a} F$, then for all R we have $P \overset{a,R}{\longmapsto} F \circ R$. If $P \overset{a,R}{\longmapsto} P'$, then there exists F such that $P \xrightarrow{a} F$ and $P' = F \circ R$.*
- *If $P \xrightarrow{\overline{a}} C$, then for all R such that $R \xrightarrow{a} F$, we have $P \overset{\overline{a},R}{\longmapsto} \equiv F \bullet C$. If $P \overset{\overline{a},R}{\longmapsto} P'$, then there exist F, C such that $P \xrightarrow{\overline{a}} C$, $R \xrightarrow{a} F$, $P' \equiv F \bullet C$.*

The correspondence is up to $\equiv$ because of scope extrusion. The contextual LTS performs scope extrusion iff the name belongs to the free names of the message, while the complementary LTS always performs scope extrusion. For instance, for $P = a(X)X \mid \nu b.\overline{a}\langle c.\mathbf{0}\rangle b.\mathbf{0}$, we have $P \xrightarrow{\tau} c.\mathbf{0} \mid \nu b.b.\mathbf{0}$ and $P \overset{\tau}{\longmapsto} \nu b.(c.\mathbf{0} \mid b.\mathbf{0})$.

4.2. Complementary Bisimilarity

We now define complementary bisimilarity and prove its soundness using Howe's method. The result in itself, i.e., the definition of a sound bisimilarity in HOπ, is far from being a new one [36, 37]. However, it allows us to explain why complementary semantics is well suited to apply Howe's method. Strong complementary bisimilarity for HOπ is simply the bisimilarity associated to the complementary LTS.

Definition 12. *Strong complementary bisimilarity $\sim_m$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P \mathcal{R} Q$ and $P \overset{\lambda}{\longmapsto} P'$ implies $Q \overset{\lambda}{\longmapsto} Q'$ with $P' \mathcal{R} Q'$.*

As in context bisimilarity, in the message output case $P \overset{\overline{a},R}{\longmapsto} P'$, the matching transition $Q \overset{\overline{a},R}{\longmapsto} Q'$ still depends on a receiving entity (here R). However, instead of considering a context which directly receives the message (an abstraction F), we consider a process R which evolves toward an abstraction. This nuance allows us to use Howe's method to prove soundness of $\sim_m$. We extend $\sim_m^\bullet$ to labels λ: we have $\lambda \sim_m^\bullet \lambda'$ iff $\lambda = \lambda' = \tau$, or $\lambda = (\gamma, R)$, $\lambda' = (\gamma, R')$ with $R \sim_m^\bullet R'$. We prove the following simulation-like property for $\sim_m^\bullet$:

Lemma 5. *Let P, Q be closed processes. If $P \sim_m^\bullet Q$ and $P \overset{\lambda}{\longmapsto} Q$, then for all $\lambda \sim_m^\bullet \lambda'$, there exists Q' such that $Q \overset{\lambda'}{\longmapsto} Q'$ and $P' \sim_m^\bullet Q'$.*

We do not have the same problem as in Section 3.3 with higher-order communication. We remind that in this case, we have $P_1 \mid P_2 \sim_m^\bullet Q_1 \mid Q_2$ with $P_1 \sim_m^\bullet Q_1$, $P_2 \sim_m^\bullet Q_2$ and $P_1 \overset{\overline{a},P_2}{\longmapsto} P'$. We can apply directly the message output clause of the induction hypothesis: there exists Q' such that $Q_1 \overset{\overline{a},Q_2}{\longmapsto} Q'$ and $P' \sim_m^\bullet Q'$. We conclude that $Q_1 \mid Q_2 \overset{\tau}{\longmapsto} Q'$ (by rule HO$^\pi$) with $P' \sim_m^\bullet Q'$ as wished.

Theorem 5. *Relation $\sim_m$ is a congruence.*

Following the correspondence result between the two LTS (Lemma 4), we now prove that the two bisimilarities are equal. The differences in the message output clauses are covered mainly with Lemma 4. The bisimilarities differ also in how they deal with input actions: complementary bisimilarity tests with a process while context bisimilarity tests with a concretion. Testing with all concretions includes tests with $\langle P \rangle \mathbf{0}$, which are the same as tests with P (up to $\equiv$). Consequently one inclusion is easy to establish:

Lemma 6. *We have $\sim \subseteq \sim_m$.*

The proof is done by showing that $\sim$ is a strong complementary bisimilarity (up to $\equiv$). The reverse inclusion requires the congruence result on $\sim_m$ (Theorem 5).

Lemma 7. *We have $\sim_m \subseteq \sim$.*

We prove the inclusion by showing that $\sim_m$ is an early strong context bisimulation (up to $\equiv$). In the message input case, we have roughly $P'\{R/X\} \sim_m Q'\{R/X\}$; by congruence it implies that $\nu\widetilde{b}.(P'\{R/X\} \mid S) \sim_m \nu\widetilde{b}.(Q'\{R/X\} \mid S)$, i.e., $(X)P' \bullet \nu\widetilde{b}.\langle R \rangle S \sim_m (X)Q' \bullet \nu\widetilde{b}.\langle R \rangle S$. With Theorem 5, tests with processes are as discriminatory as tests with concretions.

We can also define complementary semantics and bisimilarity in the weak case; see [23] for definitions and results. We give more details on the weak case for HOπP (Section 5.2).

5. Application to HOπP

5.1. Complementary LTS

As in Section 4, we define a complementary semantics which considers processes instead of abstractions in the message output case. However, there are two additional issues with HOπP. First, we have to include *bisimulation contexts* $\mathbb{E}$ since they appear in bisimilarity definitions (Definitions 7 and 8). Second, scope extrusion matters more than in HOπ, since scope of restricted names may cross locality boundaries by communication but not by structural congruence. We

$$a(X)P \overset{a,R}{\longmapsto} P\{R/X\} \quad \textsc{In}_i^p \qquad \frac{P \overset{\mu}{\mapsto} P'}{P \mid Q \overset{\mu}{\mapsto} P' \mid Q} \quad \textsc{Par}_{i\tau}^p$$

$$\frac{P \overset{\mu}{\mapsto} P'}{\nu a.P \overset{\mu}{\mapsto} \nu a.P'} \quad \textsc{Restr}_{i\tau}^p \qquad \frac{P \overset{\overline{a},P,\Box}{\longmapsto}_{\widetilde{b}} P'}{!P \overset{\tau}{\mapsto} P' \mid !P} \quad \textsc{Replic-HO}_{\tau}^p$$

$$\frac{P \overset{\mu}{\mapsto} P'}{!P \overset{\mu}{\mapsto} P' \mid !P} \quad \textsc{Replic}_{i\tau}^p \qquad \frac{P \overset{\mu}{\mapsto} P'}{a[P] \overset{\mu}{\mapsto} a[P']} \quad \textsc{Loc}_{i\tau}^p \qquad \frac{P \overset{\overline{a},Q,\Box}{\longmapsto}_{\widetilde{b}} P'}{P \mid Q \overset{\tau}{\mapsto} P'} \quad \textsc{HO}_{\tau}^p$$

Figure 4: Complementary LTS for HOπP: Internal and Message Input Actions

cannot always extrude names and still have an equivalent semantics (up to $\equiv$) as in HOπ.

We let λ range over labels of the complementary LTS. Internal actions $P \overset{\tau}{\mapsto} P'$ and message input $P \overset{a,R}{\longmapsto} P'$ are similar to the HOπ complementary transitions, except that we have to add rules for localities. We write $\overset{\mu}{\mapsto}$ for $\overset{\tau}{\mapsto} \cup \overset{a,R}{\longmapsto}$. We write $\mathrm{nbh}(\mathbb{E})$ the set of names bound by $\mathbb{E}$ at the hole position, defined inductively as follows:

$$\begin{aligned} \mathrm{nbh}(\Box) &= \emptyset \\ \mathrm{nbh}(\mathbb{E} \mid P) = \mathrm{nbh}(P \mid \mathbb{E}) &= \mathrm{nbh}(\mathbb{E}) \\ \mathrm{nbh}(a[\mathbb{E}]) &= \mathrm{nbh}(\mathbb{E}) \\ \mathrm{nbh}(\nu a.\mathbb{E}) &= \mathrm{nbh}(\mathbb{E}) \cup \{a\} \end{aligned}$$

Rules can be found in Figure 4 except for the symmetric counterpart of rules $\textsc{Par}_{i\tau}^p$ and $\textsc{HO}_{\tau}^p$. Rule $\textsc{HO}_{\tau}^p$ relies on message output transitions and is explained later. As before, we do not have a side condition on rule $\textsc{Restr}_{i\tau}^p$ because of our convention on bound and free names; if $\mu = b, R$, then we have implicitly $b \neq a$ and $a \notin \mathrm{fn}(R)$.

Output rules can be found in Figure 5, except for the symmetric of rule $\textsc{Par}_o^p$. In HOπP, context bisimilarities test a message output with an abstraction F and a bisimulation context $\mathbb{E}$. As in HOπ, output actions $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ consider a receiving process Q instead of F. We have to add contexts $\mathbb{E}$ in our labels to keep the same discriminating power, and we also use a set of names $\widetilde{b}$ to deal with scope extrusion. Transition $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ means that P is put under context $\mathbb{E}$ and emits a message on a, which is received by Q, i.e., we have $\mathbb{E}\{P\} \mid Q \overset{\tau}{\mapsto} P'$ by communication on a. In the contextual style, it means that there exists F, C such that $P \overset{\overline{a}}{\to} C$, $Q \overset{a}{\to} F$, and $P' = F \bullet \mathbb{E}\{C\}$.

Scope extrusion may happen in the process under consideration (e.g., $P = \nu c.\overline{a}\langle R\rangle S$ with $c \in \mathrm{fn}(R)$) or because of the bisimulation context $\mathbb{E}$ (e.g., $P =$

$$\frac{\mathrm{fn}(R) = \widetilde{b} \qquad Q \overset{a,R}{\longmapsto} Q' \qquad \mathrm{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset}{\overline{a}\langle R \rangle S \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} Q' \mid \mathbb{E}\{S\}} \ \textsc{Out}_o^p$$

$$\frac{\mathrm{fn}(P) = \widetilde{b} \qquad Q \overset{b,P}{\longmapsto} Q' \qquad \mathrm{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset}{b[P] \overset{\overline{b},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} Q' \mid \mathbb{E}\{\mathbf{0}\}} \ \textsc{Passiv}_o^p$$

$$\frac{P_1 \overset{\overline{a},Q,\mathbb{E}\{\Box \mid P_2\}}{\longrightarrow}_{\widetilde{b}} P'}{P_1 \mid P_2 \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'} \ \textsc{Par}_o^p \qquad \frac{P \overset{\overline{a},Q,\mathbb{E}\{\Box \mid !P\}}{\longrightarrow}_{\widetilde{b}} P'}{!P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'} \ \textsc{Replic}_o^p$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}\{b[\Box]\}}{\longrightarrow}_{\widetilde{b}} P'}{b[P] \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'} \ \textsc{Loc}_o^p \qquad \frac{P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b} \cup \{c\}} P'}{\nu c.P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \nu c.P'} \ \textsc{Extr}_o^p$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}{\longrightarrow}_{\widetilde{b}} P'}{\nu c.P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'} \ \textsc{Restr}_o^p \qquad \frac{P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'}{P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'} \ \textsc{CFree}_o^p$$

$$\frac{\begin{array}{c} c \notin \mathrm{nbh}(\mathbb{E}) \cup \mathrm{nbh}(\mathbb{F}) \\ P \overset{\overline{a},Q,\mathbb{E}\{\mathbb{F}\}}{\longmapsto}_{\widetilde{b}} P' \qquad c \in \widetilde{b} \qquad c \notin \mathrm{fn}(Q) \cup \mathrm{fn}(\mathbb{E}) \end{array}}{P \overset{\overline{a},Q,\mathbb{E}\{\nu c.\mathbb{F}\}}{\longmapsto}_{\widetilde{b}} \nu c.P'} \ \textsc{Capt}_o^p$$

Figure 5: Complementary LTS for HOπP: Message Output Actions

$\overline{a}\langle R\rangle S$ and $\mathbb{E} = d[\nu c.(\Box \mid c.\mathbf{0})]$ with $c \in \mathrm{fn}(R)$). We first define auxiliary transitions $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, where we do not allow the latter kind of capture, and we then give rules for general output transitions.

Rule $\textsc{Out}^p_o$ deals with message output $\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} \mathbb{E}\{S\} \mid Q'$. Premise $Q \overset{a,R}{\longmapsto} Q'$ checks that Q may receive R on a, and the resulting process Q' is run in parallel with the continuation S under context $\mathbb{E}$. We check that $\mathbb{E}$ does not capture free names of R with the side-condition $\mathrm{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$. We keep the free names $\widetilde{b}$ of R in the label for potential scope extrusion.

For instance, let $P = \overline{a}\langle R\rangle S$ and $c \in \mathrm{fn}(R)$. Process $\nu c.P$ may emit R on a, but the scope of c has to be expanded to encompass the recipient of R. The premise of rule $\textsc{Extr}^p_o$ checks that P may output a message; here we have $\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}}_{\mathrm{fn}(R)} \mathbb{E}\{S\} \mid Q'$. In conclusion, we have $\nu c.\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}}_{\mathrm{fn}(R)\setminus c} \nu c.(\mathbb{E}\{S\} \mid Q')$. The scope of c includes Q' as wished.

Suppose now that $P = \overline{a}\langle R\rangle S$ with $c \notin \mathrm{fn}(R)$. Process $\nu c.P$ may emit a message, but the scope of c has to encompass the continuation S only: we want to obtain $\nu c.P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} \mathbb{E}\{\nu c.S\} \mid Q'$ (with $\widetilde{b} = \mathrm{fn}(R)$). To this end, we consider $P \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}_{\widetilde{b}} P'$ as the premise of rule $\textsc{Restr}^p_o$. In process P', the continuation is put under $\mathbb{E}\{\nu c.\Box\}$, hence we obtain $\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}_{\mathrm{fn}(R)} \mathbb{E}\{\nu c.S\} \mid Q' = P'$, as expected and reflected in the conclusion of the rule. With our convention on bound and free names, the rules $\textsc{Extr}^p_o$ and $\textsc{Restr}^p_o$ do not need side-conditions on c; because c is bound in $\nu c.P$, we implicitly have $c \neq a$ and $c \notin \mathrm{fn}(Q) \cup \mathrm{fn}(\mathbb{E}) \cup \widetilde{b}$ in both rules.

Rule for passivation $\textsc{Passiv}^p_o$ is similar to rule $\textsc{Out}^p_o$, while rules $\textsc{Loc}^p_o$, $\textsc{Par}^p_o$, $\textsc{Replic}^p_o$ follow the same pattern as rule $\textsc{Restr}^p_o$. Rule $\textsc{CFree}^p_o$ simply means that a transition with a capture-free context is a message output transition. We now explain how to deal with context capture with rule $\textsc{Capt}^p_o$. Suppose $P = \overline{a}\langle R\rangle S$ and $\mathbb{E}' = d[\nu c.(\Box \mid \overline{c}\langle\mathbf{0}\rangle\mathbf{0})]$ with $c \in \mathrm{fn}(R)$; we want to obtain $P \xrightarrow{\overline{a},Q,\mathbb{E}'}_{\widetilde{b}} \nu c.(d[S \mid \overline{c}\langle\mathbf{0}\rangle\mathbf{0}] \mid Q')$ (with the scope of c extended out of d). We first consider the transition $P \xrightarrow{\overline{a},Q,\mathbb{E}\{\mathbb{F}\}}_{\widetilde{b}} P'$ without capture on c; in our case we have $P \xrightarrow{\overline{a},Q,d[\Box]}_{\widetilde{b}} d[S \mid \overline{c}\langle\mathbf{0}\rangle\mathbf{0}] \mid Q' = P'$ with $\mathbb{E} = d[\Box]$ and $\mathbb{F} = \Box \mid \overline{c}\langle\mathbf{0}\rangle\mathbf{0}$. Using the rule we have $P \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\mathbb{F}\}}_{\widetilde{b}} \nu c.P'$, i.e., $P \xrightarrow{\overline{a},Q,\mathbb{E}'}_{\widetilde{b}} \nu c.(d[S \mid \overline{c}\langle\mathbf{0}\rangle\mathbf{0}] \mid Q')$. The scope of c is extended outside $\mathbb{E}$ and includes the recipient of the message as wished.

In rule $\textsc{Capt}^p_o$, the side-condition $c \notin \mathrm{nbh}(\mathbb{E}) \cup \mathrm{nbh}(\mathbb{F})$ ensures that there is exactly one restriction on c around the hole in $\mathbb{E}\{\nu c.\mathbb{F}\}$. This is merely a convenience for certain proofs and does not impact the LTS semantics, because any context $\mathbb{E}'$ such that $c \in \mathrm{nbh}(\mathbb{E}')$ can be written $\mathbb{E}\{\nu c.\mathbb{F}\}$ with $c \notin \mathrm{nbh}(\mathbb{E}) \cup \mathrm{nbh}(\mathbb{F})$ using α-conversion for the restrictions νc which do not bind c at the hole of $\mathbb{F}$. The side-condition $c \notin \mathrm{fn}(Q) \cup \mathrm{fn}(\mathbb{E})$ in the same rule prevents unwanted captures from happening; the convention on bound and free names does not apply here, because the name c is bound at the hole position in $\mathbb{E}\{\nu c.\mathbb{F}\}$ and it

cannot be α-converted.

Premise $P \xmapsto{\overline{a},Q,\Box}_{\widetilde{b}} P'$ of rule HO^p_τ (Figure 4) means that process P sends a message on a to Q without any context around P, and the result is P'. Consequently we have $P \mid Q \overset{\tau}{\mapsto} P'$ by communication on a, which is the expected conclusion. Names $\widetilde{b}$ may no longer be potentially extruded, so we simply forget them.

5.2. Complementary Bisimilarities

We only give definitions and results, and point out the differences with HOπ (Section 4.2). In Appendix A, we prove the main results of this section in the weak case (the proofs are similar or easier in the strong case). More specifically, we prove the inclusion between weak context and complementary bisimilarity (Theorem 9), and the soundness (Theorem 8) and completeness (Theorem 10) of weak complementary bisimilarity.

Strong complementary bisimilarity is defined as follows.

Definition 13. *Strong complementary bisimilarity $\sim_m$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies $fn(P) = fn(Q)$ and for all $P \overset{\lambda}{\mapsto} P'$, there exists $Q \overset{\lambda}{\mapsto} Q'$ such that $P'\ \mathcal{R}\ Q'$.*

To prove the simulation-like result, we have to extend Howe's closure to bisimulation contexts: we define $\mathbb{E} \sim^\bullet_m \mathbb{F}$ as the smallest congruence that contains $\sim^\bullet_m$ and rule $\Box \sim^\bullet_m \Box$. Except for this point, Howe's method is easy to apply.

Theorem 6. *Relation $\sim_m$ is a congruence and is sound with respect to $\sim_b$.*

The relation is also complete, therefore we have the following equality.

Theorem 7. *We have $\sim = \sim_b$.*

Correspondence with context bisimilarity is more problematic than in HOπ. We have two major differences. First, the output clause of complementary bisimilarity requires that transition $P \xmapsto{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$ has to be matched by a transition $Q \xmapsto{\overline{a},T,\mathbb{E}}_{\widetilde{b}} Q'$ with the same set of names $\widetilde{b}$ which may be extruded. At first glance, we do not have this requirement for the early strong context bisimilarity, hence we have to prove that it is the case. For a concretion $C = \nu\widetilde{b}.\langle R\rangle S$, we define $extr(C) \triangleq \mathrm{fn}(R) \setminus \widetilde{b}$.

Lemma 8. *Let $P \sim Q$. Let $P \xrightarrow{\overline{a}} C$, F an abstraction, and $Q \xrightarrow{\overline{a}} C'$ such that for all $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \sim F \bullet \mathbb{E}\{C'\}$. Then we have $extr(C) = extr(C')$.*

Proof. Let $b, e \notin \mathrm{fn}(P, Q)$. Given two distinct names c, d, we define:

$$\mathbb{E}_{c,d} \triangleq \nu be.b[\nu c.e[\Box] \mid e(Y)(c.\mathbf{0} \mid \overline{c}.\overline{c}.d.\mathbf{0})] \mid b(Z)(Z \mid Z)$$

Suppose the scope of the name c is extruded outside b. After passivation of e and duplication of the content of b, it is possible to perform the two synchronizations

of c; the name d becomes observable. Conversely, if d becomes observable, then passivation of locality e has been triggered, and a synchronization on c is possible. Since passivation of e destroys any possible occurrence of c in e, the synchronization is possible only if the scope of c is extended outside b before duplication of the content of b. Thus, the name d becomes observable iff name c is extruded outside b.

Let $c \in extr(C)$ and d such that $d \notin \text{fn}(P, Q, F)$. Let $P' \triangleq F \bullet \mathbb{E}_{c,d}\{C\}$. We have $P' \sim F \bullet \mathbb{E}_{c,d}\{C'\} \triangleq Q'$. By definition, c is extruded outside b in P', hence name d becomes observable. Since we have $P' \sim Q'$, d becomes also observable in Q'. which is possible only if $c \in extr(C')$. Consequently we have $extr(C) \subseteq extr(C')$. Conversely let $c \in extr(C')$ and d such that $d \notin \text{fn}(P, Q, F)$. Let $P' \triangleq F \bullet \mathbb{E}_{c,d}\{C\}$. We have $P' \sim F \bullet \mathbb{E}_{c,d}\{C'\} \triangleq Q'$. With the same reasoning on Q' observables, we can prove similarly $extr(C') \subseteq extr(C)$.

□

Using Lemma 8, we have the following inclusion:

Lemma 9. *We have* $\sim \subseteq \sim_m$.

The proof is done by showing that $\sim$ is a strong complementary bisimilarity. As a direct consequence, we can deduce that $\sim$ is sound:

Corollary 1. *We have* $\sim \subseteq \sim_b$.

Moreover, if $P \sim_m Q$ and $P \overset{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$, then the matching transition $Q \overset{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} Q'$ depends on the context $\mathbb{E}$. In the context bisimilarity (Definition 7), the matching transition is independent from $\mathbb{E}$; context bisimilarity is late with respect to bisimulation contexts, while complementary bisimilarity is early with respect to these contexts. Proving that $\sim_m \subseteq \sim$ remains an open problem, but we conjecture that this inclusion holds.

Remark 9. *We can define an early context bisimilarity with respect to contexts by changing the message output clause of Definition 7 into*

- *for all* $P \xrightarrow{\overline{a}} C$*, for* $F, \mathbb{E}$*, there exists* C' *such that* $Q \xrightarrow{\overline{a}} C'$ *and* $(F \bullet \mathbb{E}\{C\})\ \mathcal{R}\ (F \bullet \mathbb{E}\{C'\})$.

We can prove that this modified bisimilarity $\sim'$ *is sound (using Kell soundness proof method) and complete (with the usual proof scheme). Consequently we have* $\sim' = \sim_b$ *and* $\sim_m = \sim_b$*, so we have* $\sim_m = \sim_b = \sim'$*. However we can prove soundness of* $\sim'$ *independently from* $\sim_m$ *only in the strong case; this reasoning cannot be applied in the weak case.*

We extend these results to the weak case. We write $\overset{\tau}{\Mapsto}$ the reflexive and transitive closure of $\overset{\tau}{\longmapsto}$. We define $\overset{a,R}{\Longmapsto}$ as $\overset{\tau}{\Mapsto}\overset{a,R}{\longmapsto}\overset{\tau}{\Mapsto}$. In the weak case, two processes P and Q may evolve independently before interacting with each other. Since a transition $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ includes a communication between P and Q, we have to authorize Q to perform τ-actions before interacting with P in the weak output transition. We define $P \overset{\overline{a},Q,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$ as $P \overset{\tau}{\Mapsto}\overset{\overline{a},Q',\mathbb{E}}{\longmapsto}_{\widetilde{b}}\overset{\tau}{\Mapsto} P'$ with $Q \overset{\tau}{\Mapsto} Q'$.

Definition 14. *Weak complementary bisimilarity $\approx_m$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies $fn(P) = fn(Q)$ and for all $P \stackrel{\lambda}{\mapsto} P'$, there exists $Q \stackrel{\hat{\lambda}}{\Rightarrow} Q'$ such that $P'\ \mathcal{R}\ Q'$.*

Using the same proof techniques as in the strong case, we have the following results:

Theorem 8. *Relation $\approx_m$ is a congruence.*

Theorem 9. *We have $\approx \subseteq \approx_m$.*

Bisimilarity $\approx_m$ coincides with $\approx_b$ on image-finite processes; a closed process P is image finite iff for every label λ, the set $\{P', P \stackrel{\hat{\lambda}}{\Rightarrow} P'\}$ is finite. Using the same proof technique as in [39], we have the following completeness result.

Theorem 10. *Let P, Q be image-finite processes. We have $P \approx_b Q$ if and only if $P \approx_m Q$.*

Complementary bisimilarity characterizes barbed congruence in the strong and weak cases. However this relation is not completely satisfactory since it tests an infinite number of environments to equate processes, especially in the message output case. The next step is to find a behavioral equivalence with fewer tests, similar to the HOπ normal bisimilarity (Section 2.2). In the following section, we give counter-examples which suggest that finding such simpler relations is not possible in HOπP.

6. Abstraction Equivalence in HOπP

In this section, we present counter-examples to show that a simplification similar to HOπ normal bisimilarity (Section 2.2) is not possible in HOπP. We prove that testing using large sub-classes of HOπP processes (the *abstraction-free* and the *finite* processes) is not enough to guarantee bisimilarity of abstraction. We first present a counter-example which relies on the chosen "by need" scope extrusion, and we then give other counter-examples which do not need this mechanism.

6.1. Abstraction-Free Processes

In the following, we omit the trailing zeros to improve readability; in an agent definition, m stands for $m.\mathbf{0}$. We also write $\nu ab.P$ for $\nu a.\nu b.P$. Let $\mathbf{0}_m \stackrel{\Delta}{=} \nu a.a.m$. Process $\mathbf{0}_m$ cannot perform any transition, like $\mathbf{0}$, but it has a free name m. We define the following abstractions:

$$(X)P \stackrel{\Delta}{=} (X)\nu nb.(b[X \mid \nu m.\overline{a}\langle \mathbf{0}_m \rangle (m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y))$$
$$(X)Q \stackrel{\Delta}{=} (X)\nu mnb.(b[X \mid \overline{a}\langle \mathbf{0} \rangle (m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y))$$

The two abstractions differ in the process emitted on a and in the position of name restriction on m (inside or outside hidden locality b). An abstraction-free

process is a process built with the regular HOπP syntax but without message input $a(X)P$.

We recall that $\sim$ is the early strong context bisimilarity (Definition 7).

Lemma 10. *Let R be an abstraction-free process. We have $(X)P \circ R \sim (X)Q \circ R$.*

Since R is abstraction-free, it cannot receive the message emitted on a; consequently R cannot interact with P or Q. Passivation of locality b (after the communication on n) and transitions from R in $(X)P \circ R$ are easily matched by the same transitions in $(X)Q \circ R$.

Let $P_{m,R} = \nu nb.(b[R \mid m \mid n \mid \overline{m}.\overline{m}.p] \mid \overline{n}.b(Y)(Y \mid Y))$, F be an abstraction, and $\mathbb{E}$ be an evaluation context such that $m \notin \text{fn}(\mathbb{E}, F)$. We now prove that $(X)P \circ R \xrightarrow{\overline{a}} \nu m.\langle \mathbf{0}_m \rangle P_{m,R}$ is matched by $(X)Q \circ R \xrightarrow{\overline{a}} \langle \mathbf{0} \rangle \nu m.P_{m,R}$, i.e., that we have $\nu m.(F \circ \mathbf{0}_m \mid \mathbb{E}\{P_{m,R}\}) \sim F \circ \mathbf{0} \mid \mathbb{E}\{\nu m.P_{m,R}\}$. Since $m \notin \text{fn}(\mathbb{E}, F)$, there is no interaction on m between $F, \mathbb{E}$, and $P_{m,R}$, and the inert process $\mathbf{0}_m$ does not interfere either. Hence the possible transitions from $\nu m.(F \circ \mathbf{0}_m \mid \mathbb{E}\{P_{m,R}\})$ are the internal ones from F and $\mathbb{E}$, interactions between F, $\mathbb{E}$, and R on names other than m, and internal actions in $P_{m,R}$. All of them are matched by the same transitions in $F \circ \mathbf{0} \mid \mathbb{E}\{\nu m.P_{m,R}\}$.

Abstractions $(X)P$ and $(X)Q$ may have different behaviors with an argument which may receive on a, like $a(Z)q$, with $p \neq q$. By communication on a, we have $(X)Q \circ a(Z)q \xrightarrow{\tau} \nu mnb.(b[q \mid m \mid n \mid \overline{m}.\overline{m}.p] \mid \overline{n}.b(Y)(Y \mid Y)) \triangleq Q_1$. Since Q_1 may perform a $\xrightarrow{q}$ transition, it can only be matched by $(X)P \circ a(Z)q \xrightarrow{\tau} \nu nb.(b[\nu m.(q \mid m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y)) \triangleq P_1$. Notice that in P_1, the restriction on m remains inside hidden locality b.

After synchronization on n and passivation/communication on b, we have $Q_1(\xrightarrow{\tau})^2 \nu mnb.(q \mid q \mid m \mid m \mid \overline{m}.\overline{m}.p \mid \overline{m}.\overline{m}.p) \triangleq Q_2$ (the process inside b in Q_1 is duplicated). After two synchronizations on m, we have $Q_2(\xrightarrow{\tau})^2 \nu mnb.(q \mid q \mid p \mid \overline{m}.\overline{m}.p) \triangleq Q_3$, and Q_3 may perform a $\xrightarrow{p}$ transition. These transitions cannot be matched by P_1. Performing the duplication, we have $P_1(\xrightarrow{\tau})^2 \nu nb.(\nu m.(q \mid m \mid \overline{m}.\overline{m}.p) \mid \nu m.(q \mid m \mid \overline{m}.\overline{m}.p)) \triangleq P_2$. Each copied sub-process $q \mid m \mid \overline{m}.\overline{m}.p$ of P_2 has its own private copy of m, and we can no longer perform any transition to have the observable p. More generally, the sequence of transitions $Q_1(\xrightarrow{\tau})^4 \xrightarrow{p}$ cannot be matched by P_1, consequently Q_1 and P_1 (and therefore $(X)Q \circ a(Z)q$ and $(X)P \circ a(Z)q$) are not bisimilar.

The previous example shows that testing abstractions with abstraction-free processes (such as $\overline{m}.\mathbf{0}$) is not enough to distinguish them. This example relies heavily on the chosen "by need" scope extrusion (restrictions are extruded outside localities along with messages only when needed), which is also used in Homer or Kell. Using a different definition of scope extrusion, for instance by considering name restriction to be a fresh name generator, is unfortunately not a solution: we present in the next section other counter-examples which do

not rely on scope extrusion yet show that testing using a large class of finite processes is not sufficient to derive abstractions equivalence.

6.2. Finite Processes

We define finite processes as follows:

Definition 15. *A finite process is a HOπP process built on the following grammar:*

$$P_F ::= \mathbf{0} \;\mid\; P_F \mid P_F \;\mid\; \nu a.P_F \;\mid\; \overline{a}\langle P\rangle P_F \;\mid\; a(X)P_F \;\mid\; a[P_F]$$

Roughly, finite processes cannot initiate an infinite sequence of transitions. Notice that in a message output, the message does not matter and can be a regular process. We do not allow process variable X in the syntax, hence finite processes encompass only message inputs $a(X)P_F$ where either $X \notin \mathrm{fv}(P_F)$ or where X appears in emitted messages only (since emitted processes in a message output may be any process). In other words, processes received on input can only be passed around but never activated. With unrestricted message input, we may encode replication (as explained in Section 2.1) and therefore have infinite sequence of transitions.

We extend the definition to all agents in the following way: a concretion $\nu\widetilde{b}.\langle R\rangle S$ is finite iff S is finite. An abstraction $(X)P$ is finite iff P is finite. We write A_F the set of finite agents. We give some properties of finite agents:

Lemma 11. *Let F be a finite abstraction. For all HOπP processes P, the process $F \circ P$ is finite.*

Let P_F be a finite process:

- *If $P_F \xrightarrow{\alpha} A$ for some α, then A is finite.*
- *The set $\{\alpha | \exists A, P_F \xrightarrow{\alpha} A\}$ is finite.*
- *For all action α, the set $\{A | P_F \xrightarrow{\alpha} A\}$ is finite.*
- *There is no infinite sequence of processes (P_i) such that $P_0 = P_F$ and for all i, $P_i \xrightarrow{\tau} P_{i+1}$ or $P_i \xrightarrow{\overline{a}} \nu\widetilde{b}.\langle R\rangle P_{i+1}$ or $P_i \xrightarrow{a} F$ with $F \circ P = P_{i+1}$ for some P.*

Since the LTS is finitely branching (second and third properties of Lemma 11) and any sequence of transitions initiated by P_F is finite, we can speak about the length of the longest sequence of transitions initiated by P_F, called *depth*.

Definition 16. *We define inductively the depth of a finite agent A_F, written $d(A_F)$, as:*

- *$d(P_F) = 0$ if there is no transition from P_F.*
- *$d(P_F) = 1 + \max\{d(A) | \exists \alpha, P_F \xrightarrow{\alpha} A\}$ otherwise.*
- *For all finite concretions $\nu\widetilde{b}.\langle P\rangle P_F$, we have $d(\nu\widetilde{b}.\langle P\rangle P_F) = d(P_F)$.*

- *For all finite abstractions $(X)P_F$, we have $d((X)P_F) = d(P_F)$.*

We may think that the depth of an abstraction depends on the interacting process. It is not the case since process variables may only occur in processes emitted in a message output, and the depth of a concretion takes into account the continuation only. Hence we have the following lemma:

Lemma 12. *Let F be a finite abstraction. For all HOπP processes P, we have $d(F \circ P) = d(F)$*

We now use depth to prove that using finite processes to test bisimilarity of abstractions is not sufficient.

6.3. Counter-examples

In this section, we give counter-examples to show that testing using finite processes is not enough to ensure bisimilarity of abstractions in HOπP (extended with a sum operator; we do not know if such a counter-example can be defined in pure HOπP). To show this, we define inductively two families of HOπP abstractions $(F_n), (G_n)$, such that for any finite process P_F with $d(P_F) \leq n$, the processes $F_n \circ P_F$ and $G_n \circ P_F$ are context bisimilar, but $F_n \circ Q_{n+1}$ and $G_n \circ Q_{n+1}$ (where Q_{n+1} is a process $m_{n+1}.\ldots.m_1.\mathbf{0}$ with $n+1$ names) are not context bisimilar. The proofs for this section can be found in Appendix B.

For a a name and $F = (X)P$ an abstraction, we write $a.F$ for $a(X)P$. We also define $\tau.P \triangleq \nu a.(\overline{a}.\mathbf{0} \mid a.P)$ (with $a \notin \mathrm{fn}(P)$). We define:

$$F_0 \triangleq (X_0)X_0$$
$$G_0 \triangleq (X_0)(X_0 \mid X_0)$$

and for $n > 0$, we define

$$F_n \triangleq (X_n)(\nu a_n.(a_n[X_n] \mid a_n.F_{n-1}) + R_n)$$
$$G_n \triangleq (X_n)(\nu a_n.(a_n[X_n] \mid a_n.G_{n-1}) + S_n)$$

with $R_n = \nu a_n.\tau.G_{n-1} \circ X_n$ and $S_n = \nu a_n.\tau.F_{n-1} \circ X_n$. Notice that R_n mimics passivation of locality a_n in G_n, and S_n mimics passivation of a_n in F_n. They have been added to match some particular transitions.

Let P_F be a finite process such that $d(P_F) \leq n$. We study first the relation between $F_n \circ P_F$ and $G_n \circ P_F$. If $n = 0$, which means that P_F cannot perform any transition, then we have to compare P_F and $P_F \mid P_F$, which are obviously bisimilar. Otherwise, we have three kinds of transitions. We consider first the transition $F_n \circ P_F \xrightarrow{\tau} \nu a_n.G_{n-1} \circ P_F$, which comes from the sub-process R_n. This transition is easily matched by the passivation of locality a_n in $G_n \circ P_F$: we have $G_n \circ P_F \xrightarrow{\tau} \nu a_n.G_{n-1} \circ P_F$, the two obtained processes are identical. Similarly, we have $F_n \circ P_F \xrightarrow{\tau} \nu a_n.F_{n-1} \circ P_F$ by passivation of locality a_n;

$G_n \circ P_F$ matches this transition by the τ-action $G_n \circ P_F \xrightarrow{\tau} \nu a_n.F_{n-1} \circ P_F$ from the sub-process S_n.

The last kind of evolutions from the process $F_n \circ P_F$ is the succession of one or several transitions from P_F, followed by passivation of a_n. Roughly we have $F_n \circ P_F \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_k} \nu a_n.(a_n[P'_F] \mid a_n.F_{n-1}) \xrightarrow{\tau} \nu a_n.(F_{n-1} \circ P'_F)$, with $d(P'_F) \leq n-1$. It can be matched by the same transitions in $G_n \circ P_F$; we have $G_n \circ P_F \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_k} \nu a_n.(a_n[P'_F] \mid a_n.G_{n-1}) \xrightarrow{\tau} \nu a_n.(G_{n-1} \circ P'_F)$. Hence we obtain two processes bisimilar to $F_{n-1} \circ P'_F$ and $G_{n-1} \circ P'_F$ with $d(P'_F) \leq n-1$ Consequently, we can prove the following lemma by induction on n:

Lemma 13. *If $d(P_F) \leq n$, then $F_n \circ P_F \sim G_n \circ P_F$.*

Now, we consider (m_k) a family of pairwise distinct fresh names which do not occur in any F_n nor G_n. Let $Q_1 = m_1.\mathbf{0}$ and $Q_{k+1} = m_{k+1}.Q_k$ for all $k > 1$. We explain why $F_n \circ Q_{n+1}$ and $G_n \circ Q_{n+1}$ are not bisimilar. Consider the following sequence of transitions from $F_n \circ Q_{n+1}$: an $\xrightarrow{m_{n+1}}$ transition, followed by a passivation of locality a_n; we obtain $F_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.F_{n-1}) \xrightarrow{\tau} \sim F_{n-1} \circ Q_n$. As this sequence must be matched by $G_n \circ Q_{n+1}$, in particular the initial $\xrightarrow{m_{n+1}}$ transition that selects the left process in the choice, we obtain $F_{n-1} \circ Q_n$ and $G_{n-1} \circ Q_n$. After repeating this sequence of transitions $n-1$ times, we obtain $F_0 \circ Q_1 = m_1.\mathbf{0}$ and $G_0 \circ Q_1 = m_1.\mathbf{0} \mid m_1.\mathbf{0}$, which are clearly not bisimilar. Consequently $F_n \circ Q_{n+1}$ is not bisimilar to $G_n \circ Q_{n+1}$.

To summarize, testing using a finite process P_F with depth n is not enough, since we have $F_n \circ P_F \sim G_n \circ P_F$, but $F_n \circ Q_{n+1} \nsim G_n \circ Q_{n+1}$. Testing using a finite set $\mathcal{P}$ of finite processes is not enough either. Since $\mathcal{P}$ is finite, the set $\{d(P_F) | P_F \in \mathcal{P}\}$ is finite and has a greatest element d. For all $P_F \in \mathcal{P}$, we have $F_d \circ P_F \sim G_d \circ P_F$ but $F_d \circ Q_{d+1} \nsim F_d \circ Q_{d+1}$. Similarly, testing using an infinite set of finite processes with depths bounded by d is not enough.

Finite processes allow for very limited inputs, therefore most finite processes are abstraction-free processes, and are already covered by the abstraction-free counter-example. However, the finite processes counter-examples do not rely on scope extrusion "by need" like the previous one, which means that they may still be valid with other ways to handle scope extrusion. However, both counter-examples are not definitive enough to state that we cannot define an equivalence which tests only a finite set of processes at each bisimulation step; the problem remains open. We can however define a normal bisimilarity if we remove the restriction operator from HOπP, as explained in the following section.

7. Normal Bisimilarities in HOP

We now develop a full behavioral theory for HOP, a calculus with passivation but without restriction: we define higher-order and normal bisimilarities which characterize barbed congruence in both strong and weak cases. HOP (for Higher Order with Passivation) is the calculus obtained by removing restriction from

HOπP and adding a sum operator (to obtain the characterization result, since + is needed to show the completeness of HO bisimilarity and requires restriction to be faithfully encoded). The LTS contextual rules for HOP are the same as the HOπP ones, with the addition of the rule

$$\frac{P \xrightarrow{\alpha} A}{P + Q \xrightarrow{\alpha} A} \text{ SUM}$$

and of its symmetric rule. The structural congruence rules for HOP, also written $\equiv$, is the smallest congruence that verifies the following laws.

$$P \mid (Q \mid R) \equiv (P \mid Q) \mid R \qquad P \mid Q \equiv Q \mid P \qquad P \mid \mathbf{0} \equiv P$$

$$P + (Q + R) \equiv (P + Q) + R \qquad P + Q \equiv Q + P \qquad P + \mathbf{0} \equiv P \qquad !P \equiv P \mid !P$$

Even without restriction, HOP remains quite expressive since it is an extension of the Turing-complete HOcore calculus defined in [21].

7.1. HO Bisimulation

We first give an LTS-based characterization of strong barbed congruence (Definition 1). As pointed out in Section 2.4, a message and its continuation may be put in different contexts because of passivation. Moreover, they are completely independent since they no longer share private names, as there is no restriction. Instead of keeping them together, we can now study them separately and still have a sound and complete bisimilarity. We propose the following bisimulation, called HO bisimulation, similar to the higher-order bisimulation given by Thomsen for Plain CHOCS [43].

Definition 17. *Early strong HO bisimilarity, written $\dot{\sim}$, is the largest symmetric relation $\mathcal{R}$ such that $P \mathcal{R} Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathcal{R} Q'$.*
- *for all $P \xrightarrow{a} F$, for all closed processes R, there exists F' such that $Q \xrightarrow{a} F'$ and $F \circ R \mathcal{R} F' \circ R$.*
- *for all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$, $R \mathcal{R} R'$, and $S \mathcal{R} S'$.*

In the following we also use the late counterpart of HO bisimilarity, written $\dot{\sim}_l$, which is obtained by replacing the input case by:

- For all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and for all closed processes R, $F \circ R \mathcal{R} F' \circ R$.

We show later that early and late HO bisimilarities coincide (as in HOπ). Howe's method works with $\dot{\sim}_l$; there is no need to define a complementary semantics.

Theorem 11. *We have $P \dot{\sim}_l Q$ iff P and Q are strong barbed congruent.*

We define early weak (non-delay) HO bisimulation as:

Definition 18. *Early weak HO bisimilarity, written $\dot{\approx}$, is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P \mathcal{R} Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \mathcal{R} Q'$.*
- *for all $P \xrightarrow{a} F$, for all closed processes R, there exist F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ R \stackrel{\tau}{\Rightarrow} Q'$, and $F \circ R \mathcal{R} Q'$.*
- *for all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exist R', S'', S' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $R \mathcal{R} R'$, and $S \mathcal{R} S'$.*

We define late weak HO bisimilarity, written $\dot{\approx}_l$, by replacing the input clause by:

- for all $P \xrightarrow{a} F$, there exists F' such that $Q \stackrel{a}{\Rightarrow} F'$ and for all closed processes R, there exists Q' such that $F' \circ R \stackrel{\tau}{\Rightarrow} Q'$ and $F \circ R \mathcal{R} Q'$.

As in the strong case, we prove soundness of $\dot{\approx}$ using Howe's method.

Theorem 12. *If $P \dot{\approx} Q$, then P and Q are weak barbed congruent.*

We prove completeness on *image-finite* processes. A HOP process P is image finite iff for all α, the set $\{A | P \stackrel{\alpha}{\Rightarrow} A\}$ is finite.

Theorem 13. *Let P, Q be image finite processes. If P, Q are weak barbed congruent, then they are early weak HO bisimilar.*

We note that the definitions of higher-order bisimulations are easier to use since there is no universal quantification in the concretion case. In the following subsection, we show that the one in the abstraction case is not necessary.

7.2. Normal Bisimulation

In this section, we define a sound and complete bisimulation for the strong and weak cases without any universal quantification, similar to HOπ normal bisimulation [37]. Sangiorgi first defined it in the weak case, and then Cao extended it to the strong case [6]. In Appendix C, we prove the main results (Lemma 14 and Theorem 14) in the strong case; the proof is similar in the weak case.

In the message input case, HOπ normal bisimulation tests abstractions with only one trigger $m.\mathbf{0}$, where m is a fresh name. This testing is not sufficient in HOP. Consider the following processes:

$$P_1 \triangleq !a[X] \mid !a[\mathbf{0}] \qquad Q_1 \triangleq X \mid P_1$$

Let $P_m \triangleq P_1\{m.\mathbf{0}/X\}$, $Q_m \triangleq Q_1\{m.\mathbf{0}/X\}$, $P_{m,n} \triangleq P_1\{m.n.\mathbf{0}/X\}$, and $Q_{m,n} \triangleq Q_1\{m.n.\mathbf{0}/X\}$, where m, n do not occur in P_1, Q_1.

We first prove that $P_m \dot{\sim}_l Q_m$. Since the other transitions are easily matched, we consider only the move $Q_m \xrightarrow{m} \mathbf{0} \mid P_m$. It can only be matched by a replicated locality $a[m.\mathbf{0}]$; we have $P_m \xrightarrow{m} a[\mathbf{0}] \mid P_m$. The two resulting processes $\mathbf{0} \mid P_m$ and $a[\mathbf{0}] \mid P_m$ are immediately bisimilar, due to the presence of $!a[\mathbf{0}]$ in P_m. Consequently we have $P_m \dot{\sim}_l Q_m$.

However we have $P_{m,n} \not\dot{\sim}_l Q_{m,n}$. Indeed, the transition $Q_{m,n} \xrightarrow{m} n.\mathbf{0} \mid P_{m,n} \triangleq Q'_{m,n}$ can only be matched by $P_{m,n} \xrightarrow{m} a[n.\mathbf{0}] \mid P_{m,n} \triangleq P'_{m,n}$. Processes $P'_{m,n}$ and $Q'_{m,n}$ are not HO bisimilar: by passivation of locality $a[n.\mathbf{0}]$, we have $P'_{m,n} \xrightarrow{\overline{a}} \langle n.\mathbf{0}\rangle P_{m,n}$, which can only be matched by $Q'_{m,n} \xrightarrow{\overline{a}} \langle m.n.\mathbf{0}\rangle Q'_{m,n}$ or $Q'_{m,n} \xrightarrow{\overline{a}} \langle \mathbf{0}\rangle Q'_{m,n}$. The emitted processes are not pairwise HO bisimilar, consequently we have $P'_{m,n} \not\dot{\sim}_l Q'_{m,n}$.

One could argue that the weakness of the distinguishing power of the trigger $m.\mathbf{0}$ is due to the fact that localities are completely transparent, thus the provenance of a message may not be directly observed. However, the existence of localities around a message has indirect effects, when passivation transforms an evaluation context (the locality) into a message that may be discarded. Triggers of the form $m.n.\mathbf{0}$ allow the observation of an evaluation context (there is an emission on m) that disappears (there is no further emission on n), thus the presence of enclosing localities.

We now generalize this idea to show that it may be used to pinpoint the position of a process variable in the locality tree. Suppose we have $P\{m.n.\mathbf{0}/X\}$ bisimilar to $Q\{m.n.\mathbf{0}/X\}$, with m, n not occurring in P, Q. Suppose further that $P \xrightarrow{m} P'$ is matched by $Q \xrightarrow{m} Q'$. The processes P', Q' may now perform one and only one $\xrightarrow{n}$ transition from the single process $n.\mathbf{0}$. Now suppose that $n.\mathbf{0}$ is in a locality a in P'. Passivation of this locality results in a concretion whose message R is such that $R \xrightarrow{n}$. The process Q' has to match these transitions with $Q' \xrightarrow{\overline{a}} \langle R'\rangle S'$ such that $R \dot{\sim}_l R'$. Since $R \xrightarrow{n}$, we have $R' \xrightarrow{n}$; it is possible if and only if the single occurrence of $n.\mathbf{0}$ in Q' was in a locality a. With the same argument on R, R', we prove that the locality hierarchies around $n.\mathbf{0}$ in P' and Q' are the same. This result is formalized by the following lemma:

Lemma 14. *Let P, Q such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/Y\} \triangleq P_n$ matched by $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/Y\} \triangleq Q_n$ with $P_n \dot{\sim}_l Q_n$.*

There exist $k \geq 0$, $a_1, \ldots a_k$, $P_1 \ldots P_{k+1}$, $Q_1 \ldots Q_{k+1}$ such that either $P_n \equiv n.\mathbf{0} \mid P_1$ and $Q_n \equiv n.\mathbf{0} \mid Q_1$ or

$$\begin{aligned} P_n &\equiv a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \ldots] \mid P_1 \\ Q_n &\equiv a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \ldots] \mid Q_1 \end{aligned}$$

and for all $1 \leq j \leq k+1$, $P_j \dot{\sim}_l Q_j$.

The lemma allows us to decompose P_n, Q_n in bisimilar sub-processes. For instance, if we have $P_n \equiv a[b[n.\mathbf{0} \mid P_3] \mid P_2] \mid P_1$ with $P_n \dot{\sim}_l Q_n$, then $Q_n \equiv$

$a[b[n.\mathbf{0} \mid Q_3] \mid Q_2] \mid Q_1$ with $P_1 \dot{\sim}_l Q_1$, $P_2 \dot{\sim}_l Q_2$, and $P_3 \dot{\sim}_l Q_3$. Note that we do not decompose the initial processes P and Q themselves, but this result is enough to prove the following theorem:

Theorem 14. *Let P, Q two processes such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. If $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, then for all closed processes R, we have $P\{R/X\} \dot{\sim}_l Q\{R/X\}$*

We sketch the proof of Theorem 14 to explain how Lemma 14 is used.

Sketch. We show that the symmetric closure of the relation

$$\mathcal{R} \triangleq \{(P\{R/X\}, Q\{R/X\}) \mid P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}, m, n \text{ not in } P, Q\}$$

is a late HO bisimulation. It is done by case analysis on the transition performed by $P\{R/X\}$. Suppose we have $P\{R/X\} \xrightarrow{\tau} P'\{R'/X_i\}\{R/X\}$, i.e., a copy of R (at position X_i) performs a transition $R \xrightarrow{\tau} R'$. Occurrence X_i is in an evaluation context, so we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{n.\mathbf{0}/X_i\}\{m.n.\mathbf{0}/X\} = P'_n$, matched by $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{n.\mathbf{0}/X_j\}\{m.n.\mathbf{0}/X\} = Q'_n$ with $P'_n \dot{\sim}_l Q'_n$. As X_j is also in an evaluation context, we have $Q\{R/X\} \xrightarrow{\tau} Q'\{R'/X_j\}\{R/X\}$. We now have to prove that $P'\{R'/X_i\}\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q'\{R'/X_j\}\{m.n.\mathbf{0}/X\}$.

Lemma 14 allows us to write $P'_n \equiv a_1[\ldots a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k \ldots] \mid P_1$ and $Q'_n \equiv a_1[\ldots a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k \ldots] \mid Q_1$ with $(P_r), (Q_r)$ pairwise bisimilar processes for $r \in \{1 \ldots k+1\}$. Since $P_{k+1} \dot{\sim}_l Q_{k+1}$ and $\dot{\sim}_l$ is sound, we have $a_k[R' \mid P_{k+1}] \dot{\sim}_l a_k[R' \mid Q_{k+1}]$. By induction on $r \in \{k \ldots 1\}$, we prove that $a_r[\ldots a_k[R' \mid P_{k+1}] \mid P_k \ldots] \mid P_j \dot{\sim}_l a_r[\ldots a_k[R' \mid Q_{k+1}] \mid Q_k \ldots] \mid Q_j$, obtaining $P'\{R'/X_i\}\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q'\{R'/X_j\}\{m.n.\mathbf{0}/X\}$ (for $r = 1$) as needed. □

Using this result we define a normal bisimulation for HOP:

Definition 19. *Strong normal bisimilarity $\dot{\sim}_n$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P \mathcal{R} Q$ implies :*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathcal{R} Q'$.*
- *for all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and for two names m, n which do not occur in processes P, Q, we have $F \circ m.n.\mathbf{0} \mathcal{R} F' \circ m.n.\mathbf{0}$.*
- *for all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$, $R \mathcal{R} R'$ and $S \mathcal{R} S'$.*

As a corollary of Theorem 14, we have

Corollary 2. $\dot{\sim}_l = \dot{\sim}_n = \dot{\sim}$.

By definition, we have $\dot{\sim}_l \subseteq \dot{\sim} \subseteq \dot{\sim}_n$. The inclusion $\dot{\sim}_n \subseteq \dot{\sim}_l$ is a consequence of Theorem 14.

Weak normal bisimilarity that coincides with weak HO bisimilarity may also be defined.

Definition 20. *Weak normal bisimilarity $\dot{\approx}_n$ is the largest symmetric relation on closed processes $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$ implies:*

- *for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *for all $P \xrightarrow{a} F$, there exists G such that $Q \stackrel{a}{\Rightarrow} F'$ and for two names m, n which do not occur in processes P, Q, there exists Q' such that $F' \circ m.n.\mathbf{0} \stackrel{\tau}{\Rightarrow} Q'$ and $F \circ m.n.\mathbf{0}\ \mathcal{R}\ Q'$.*
- *for all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S'', S' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $R\ \mathcal{R}\ R'$ and $S\ \mathcal{R}\ S'$.*

Theorem 15. $\dot{\approx}_n = \dot{\approx} = \dot{\approx}_l$

The proof technique is similar to the strong case and relies on weak versions of Theorem 14 and Lemma 14. Hence in a calculus with passivation and without restriction, we can define a suitable bisimulation without any universal quantification in the strong and weak cases.

8. Related work

Behavioral equivalences in higher-order calculi. Very few higher-order calculi feature a coinductive characterization of weak barbed congruence, let alone one with finite testing, similar to normal bisimilarity. It is the case in HOπ (discussed in Section 2.1), and in a fragment of concurrent ML with local names [19]. In both calculi, normal bisimilarity comes from a triggered semantics, where triggers are passed instead of processes, which equates the "regular" semantics in the weak case. Cao [6] has extended HOπ normal bisimilarity to the strong case.

HOcore [21] is a minimal higher-order calculus (without any restriction or replication constructors), with various characterizations of strong barbed congruence, including higher-order and normal ones. Lanese et al. also give an axiomatization for bisimilarity, which shows that a behavioral equivalence in HOcore is in fact very discriminating. The authors do not know if their results holds in the weak case or when replication is added to the calculus.

Mobile Ambients [8] is a calculus with hierarchical localities and subjective linear process mobility. Localities, called *ambients*, may move by themselves in the locality hierarchy, without any acknowledgement from their environment, but they cannot be duplicated. Contextual characterizations of weak barbed congruence have been defined for Mobile Ambients [29] and its variant NBA [5]. A normal characterization has yet to be found in both calculi.

Difficulties arise in more expressive process calculi. The Seal calculus [10] is a calculus with objective process mobility which allows more flexibility than Mobile Ambients; in particular localities may be stopped, and duplicated. Process mobility requires synchronization between three processes (a process sending a name a, a receiving process, and a locality named a). The authors define a weak delay context bisimilarity in [10] called *Hoe bisimilarity* for the Seal calculus and prove its soundness. The authors point out that Hoe bisimilarity is

not complete, not only because of the delay style, but also because of the labels introduced for partial synchronization which are most likely not all observable.

The Kell calculus [41] and Homer [17] are two higher-order calculi featuring a more general process mobility called passivation or active mobility. The two calculi differ in how they handle communication; in particular, the Kell calculus allows join patterns while Homer does not. Sound and complete contexts bisimilarities have been defined for both calculi in the strong case. As stated before, a weak delay input-early bisimilarity has been proven sound in Homer using Howe's method.

Congruence proof method. In [28], Li and Liu propose a labelled transition system and a strong bisimilarity similar to the complementary semantics for HOπ (Section 4). However, they do not use Howe's method to prove congruence of the bisimilarity; instead they use an ad hoc method which relies on the factorization theorem (Theorem 4). A factorization theorem is a property stronger than congruence, and calculi featuring such a result are the exceptions, not the rule. Therefore Li and Liu congruence proof method probably cannot be used for other process calculi.

Howe's method has been originally used to prove congruence in a lazy functional programming language [18]. Baldamus and Frauenstein [2] are the first to adapt the method to process calculi for variants of Plain CHOCS [43]. They prove congruence of a late delay context bisimilarity in a calculus with static scoping, and then use it for late and early delay higher-order bisimilarities in a calculus with dynamic scoping, where emitted messages may escape the scope of their restricted names. Hildebrandt and Godskesen adapt Howe's method for their calculus Homer [17]. As already explained through this paper, they prove congruence for late delay [17] and input-early delay [14] context bisimilarities.

In [38], Sangiorgi et al. propose *environmental bisimilarity* for several higher-order languages, including HOπ. The idea is to compare P and Q using an environment $\mathcal{E}$, which represents the knowledge that an observer has about these processes. This environment contains for instance the processes emitted by P and Q. The observer uses the environment to challenge P and Q. For instance, the observer is able to compare inputs from P and Q with any messages built from the processes inside $\mathcal{E}$. Environmental bisimilarity characterizes barbed congruence in HOπ. More recently, Piérard and Sumii developed environmental bisimulations for HOπP [33]. Their approach is not complete, seemingly because of the interplay between "by need" scope extrusion and passivation, but as they show it may be applied "up to context", it potentially simplifies some bisimilarity proofs.

Instead of proving directly congruence of the bisimilarity, it is possible to design the LTS so that the associated bisimilarity is automatically a congruence. We briefly mention three methods which rely on this principle. A first method is to respect some LTS *rule format* that guarantees that the corresponding bisimilarity is a congruence. Checking that a LTS follows a given format is usually simpler than proving congruence directly. For higher-order calculi, Mousavi et al. [32] propose the Promoted and Higher-Order PANTH formats.

The Promoted PANTH format guarantees that the regular bisimilarity (where an action is matched by exactly the same action) associated to the LTS is a congruence, and the Higher-Order PANTH format guarantees that the higher-order bisimilarity (where a higher-order action is matched by a bisimilar one, as in Section 7.1) is a congruence. However, these formats can be used for strong bisimilarities only. Furthermore, they exclude side-conditions on names (such as $a \in \mathrm{fn}(R)$), making lazy scope extrusion (as in HOπP) impossible to write. Some rule formats that handle name bindings have been defined in [45, 11] for first-order process calculi; it would be interesting to combine the PANTH formats with these systems to be able to deal with lazy scope extrusion in higher-order calculi.

In [34, 35], the LTS rules are automatically derived from the reduction rules and observable so that the associated bisimilarity is a congruence. Reduction rules are decomposed in order to identify the reacting sub-term and the context the environment has to provide to trigger the reduction. The method has been applied to the π-calculus [34], HOπ [34], and the Ambients [35], but only to prove congruence of strong bisimilarities. We do not know if the method works for weak ones.

Process calculi can be viewed as *reactive systems*, where transitions from a term $\mathbb{C}\{P\}$ to P' are written $P \xrightarrow{\mathbb{C}} P'$. The main goal is then to find the minimal context $\mathbb{C}$ such that an interaction with P is possible. Bonchi et al. [4] propose a LTS derived from reactive systems for the Ambients, and use barbed bisimilarities to characterize strong and weak barbed congruence. We do not know if it is possible to encode calculi with passivation as reactive systems.

9. Conclusions and Future Work

Behavioral theory in calculi with passivation (like the Kell calculus or Homer) is less developed than the HOπ one. They are equipped with a sound and complete context bisimulation in the strong case only, which features additional tests on contexts in the message output case. Using HOπP, a higher-order calculus with passivation, we explain why usual congruence proof methods fail in the weak case in calculi with passivation. In particular, we explain that Howe's method cannot be applied to early context bisimilarities because of the interdependency between the message input and message output clauses. To overcome this difficulty, we define a complementary labelled transition system where message outputs do not depend on an abstraction, but on a process which evolves to an abstraction. This modification allows to use the Howe's method to prove congruence in the strong and weak cases.

We define a complementary semantics for HOπ and HOπP (and also for the Seal [10] in [23]). In HOπ, the complementary semantics is sound and complete, and coincides with early context bisimilarity. We obtain similar results in HOπP, except we only have one inclusion instead of equality between the relations; we conjecture that they are indeed equal. We also define a complementary semantics for the Kell in [22], with mixed results. The main issue is dealing

with join patterns. To complement an emitting process P, we need a receiving process Q, but also other emitting processes $\widetilde{R}$ to match the receiving pattern of Q. We cope with this difficulty by progressively instantiating the pattern of Q: to receive n messages, we use n transitions instead of one. To apply the Howe's method, we have to consider the bisimilarity which relates partially instantiated inputs. As a result, we obtain a sound but not complete bisimilarity in the weak case. Nevertheless, we believe it is possible to define a sound and complete complementary bisimilarity in a Kell variant without join patterns or in Homer.

The crucial step in defining a complementary semantics for a given calculus is the definition of the transition rules, especially the message output ones. If these rules are written under some restrictions, the congruence proof of the associated bisimilarity is straightforward. A future work would be to make these restrictions explicit. For instance, the classical rule for replication

$$\frac{P \mid !P \xrightarrow{\alpha} A}{!P \xrightarrow{\alpha} A}$$

makes inductive proofs of the Howe's method fails, because $P \mid !P$ in the premise is not a subterm of the process $!P$ in the conclusion. Identifying all these constraints can lead to the definition of a rule format which guarantees the soundness of the associated complementary bisimilarity, similar to the Promoted or Higher-Order PANTH format for higher-order calculi [32].

We also plan to study complementary bisimilarities defined with the regular contextual semantics. As mentioned before, in Kell (and more generally, in calculi with join-patterns), it is not possible to define a satisfactory complementary semantics; the associated bisimilarity is not complete. We want to come back to contextual semantics in order to fix this issue. It means that we change the message output clause of the early context bisimilarity such that the matching transition depends on a process, and not on an abstraction. For instance in HOπ, we have to consider the following clause:

- If $P \xrightarrow{\overline{a}} C$, then for all process R, there exists C' such that $Q \xrightarrow{\overline{a}} C'$, and for all F such that $R \xrightarrow{a} F$, we have $F \bullet C \mathcal{R} F \bullet C'$.

The corresponding relation is not completely early, because the matching transition does not depend on an abstraction F, but it is not late either, because the transition depends on a process R. We believe we can prove directly soundness of this "between late and early" bisimilarity with Howe's method, and we hope we can use this technique to obtain a characterization result in the weak case for the Kell.

Complementary and context bisimilarities are not completely satisfactory as substitutes for barbed congruence, since they reduce only slightly the quantifications. The following step is to find a characterization with fewer quantifications, similar to normal bisimilarity in HOπ. We give counterexamples which suggest

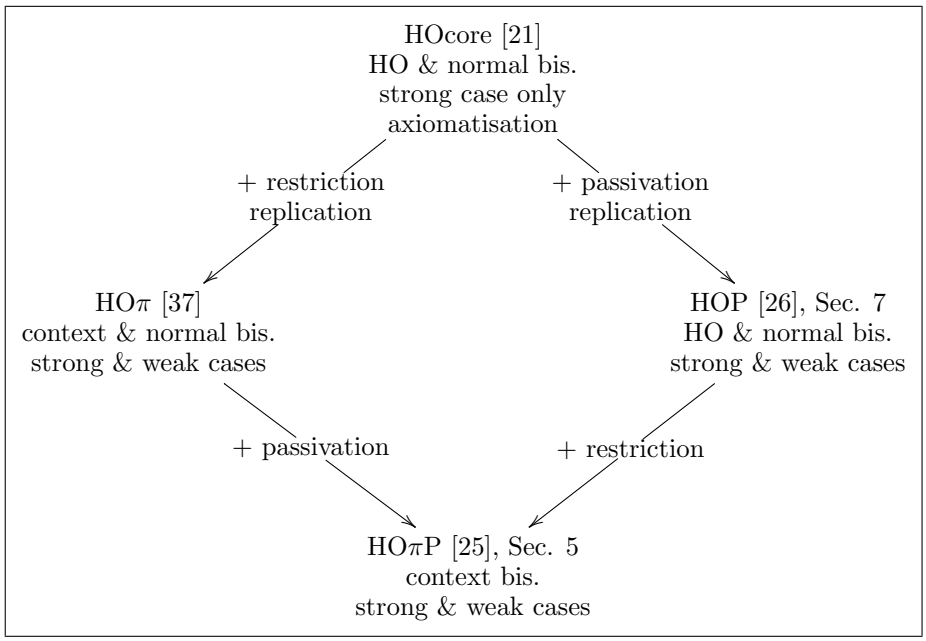


Figure 6: Characterizations results in some simple higher-order calculi

that it is not possible to find such relations in HOπP. We conjecture that in a calculus featuring passivation and name restriction, we cannot define a sound and complete strong bisimilarity with fewer tests than in Definition 7. We are however able to define such relation in HOP, a calculus with passivation but without restriction. In the case of HOπ, normal bisimulation comes from an encoding of higher-order processes into first-order ones, which is not possible in HOP. Instead, normal bisimulation in HOP relies on some means (a process $m.n.\mathbf{0}$) to observe locality hierarchies and to decompose abstractions in bisimilar sub-processes. We wonder if we can go further, and define an axiomatisation of barbed congruence in HOP. We plan to study a minimal calculus with passivation (simpler than HOP) to see if we can obtain an axiomatisation result similar to the HOcore one [21].

Finally, we obtain very different characterization results in HOπP and HOP, the two calculi with passivation we have studied in this paper. We summarize our results and compare them to results in similar calculi in Figure 6. Passivation in itself is not a problem when defining behavioral equivalences; the additional complexity previously observed in calculi such as Homer or Kell comes from the interaction between passivation and restriction.

[1] M. Baldamus. *Semantics and Logic of Higher-Order Processes: Characterizing Late Context Bisimulation*. PhD thesis, Berlin University of Technology, 1998.

[2] M. Baldamus and T. Frauenstein. Congruence proofs for weak bisimulation equivalences on higher–order process calculi. Technical report, Berlin University of Technology, 1995.

[3] M. Baldi and G. P. Picco. Evaluating the Tradeoffs of Mobile Code Design Paradigms in Network Management Applications. In *20th International Conference on Software Engineering (ICSE'97)*. IEEE, 1998.

[4] F. Bonchi, F. Gadducci, and G.V. Monreale. Reactive systems, barbed semantics, and the mobile ambients. In *FOSSACS '09*, pages 272–287. Springer, 2009.

[5] M. Bugliesi, S. Crafa, M. Merro, and V. Sassone. Communication and mobility control in boxed ambients. *Information and Computation*, 202, 2005.

[6] Z. Cao. More on bisimulations for higher order pi-calculus. In *FoSSaCS '06*, volume 3921 of *LNCS*, pages 63–78. Springer, 2006.

[7] L. Cardelli. A language with distributed scope. *Computing Systems Vol. 8 No. 1*, 1995.

[8] L. Cardelli and A. D. Gordon. Mobile ambients. In *FoSSaCS '98*, volume 1378 of *LNCS*, pages 140–155. Springer, 1998.

[9] A. Carzaniga, G. P. Picco, and G. Vigna. Designing Distributed Applications with Mobile Code Paradigms. In *19th International Conference on Software Engineering (ICSE'97)*. IEEE, 1997.

[10] G. Castagna, J. Vitek, and F. Zappa Nardelli. The Seal Calculus. *Information and Computation*, 201(1):1–54, 2005.

[11] M. P. Fiore and S. Staton. A congruence rule format for name-passing process calculi. *Inf. Comput.*, 207(2):209–236, 2009.

[12] C. Fournet, F. Le Fessant, L. Maranget, and A. Schmitt. JoCaml: a language for concurrent, distributed and mobile programming. In *Summer Schol Adv. Functional Programming*, volume 2638 of *LNCS*, 2003.

[13] A. Fuggetta, G. P. Picco, and G. Vigna. Understanding Code Mobility. *IEEE Trans. Software Eng.*, 24(5), 1998.

[14] J. C. Godskesen and T. Hildebrandt. Extending howe's method to early bisimulations for typed mobile embedded resources with local names. In *FSTTCS '05*, volume 3821 of *LNCS*, pages 140–151. Springer, 2005.

[15] A. D. Gordon. Bisimilarity as a theory of functional programming. Minicourse. Notes Series NS-95-3, BRICS, University of Cambridge Computer Laboratory, July 1995. iv+59 pp.

[16] M. Hennessy, J. Rathke, and N. Yoshida. Safedpi: a language for controlling mobile code. *Acta Inf.*, 42(4-5), 2005.

[17] T. Hildebrandt, J. C. Godskesen, and M. Bundgaard. Bisimulation congruences for Homer — a calculus of higher order mobile embedded resources. Technical Report ITU-TR-2004-52, IT University of Copenhagen, 2004.

[18] D. J. Howe. Proving congruence of bisimulation in functional programming languages. *Information and Computation*, 124(2):103–112, 1996.

[19] A. Jeffrey and J. Rathke. A theory of bisimulation for a fragment of concurrent ML with local names. *Theoretical Computer Science*, 323:1–48, 2004.

[20] A. Jeffrey and J. Rathke. Contextual equivalence for higher-order pi-calculus revisited. *Logical Methods in Computer Science*, 1(1), 2005.

[21] I. Lanese, J. A. Pérez, D. Sangiorgi, and A. Schmitt. On the expressiveness and decidability of higher-order process calculi. In *LICS*, pages 145–155. IEEE Computer Society, 2008.

[22] S. Lenglet. *Bisimulations dans les calculs avec passivation.* PhD thesis, Université de Grenoble, 2010.

[23] S. Lenglet, A. Schmitt, and J.-B. Stefani. Howe's method for early bisimilarities. Technical Report RR 6773, INRIA, 2008.

[24] S. Lenglet, A. Schmitt, and J.-B. Stefani. Normal bisimulations in process calculi with passivation. Technical Report RR 6664, INRIA, 2008.

[25] S. Lenglet, A. Schmitt, and J.-B. Stefani. Howe's method in calculi with passivation. In *CONCUR '09*, volume 5710 of *LNCS*, pages 448–462. Springer, 2009.

[26] S. Lenglet, A. Schmitt, and J.-B. Stefani. Normal bisimulations in process calculi with passivation. In *FoSSaCS '09*, volume 5504 of *LNCS*, pages 257–271. Springer, 2009.

[27] J.-J. Levy. Some results in the join-calculus. *Lecture Notes in Computer Science*, 1281:233+, 1997.

[28] Y. Li and X. Liu. Towards a theory of bisimulation for the higher-order process calculi. *Journal of Computer Science and Technology*, 19(3):352–363, 2004.

[29] M. Merro and F. Zappa Nardelli. Behavioral theory for mobile ambients. *Journal of the ACM*, 52(6):961–1023, 2005.

[30] R. Milner. *Communicating and Mobile Systems : the π-calculus.* Cambridge University Press, 1999.

[31] R. Milner and D. Sangiorgi. Techniques of weak bisimulation up-to. In *CONCUR '92*, volume 630 of *LNCS*, 1992.

[32] M. Mousavi, M. J. Gabbay, and M. A. Reniers. Sos for higher order processes (extended abstract). In *CONCUR'05*, volume 3653 of *LNCS*, pages 308–322. Springer, 2005.

[33] Adrien Piérard and Eijiro Sumii. Sound bisimulations for higher-order distributed process calculus. In Martin Hofmann, editor, *FOSSACS '11*, volume 6604 of *Lecture Notes in Computer Science*, pages 123–137. Springer, 2011.

[34] J. Rathke and P. Sobocinski. Deconstructing behavioural theories of mobility. In *IFIP TCS '08*, volume 273 of *IFIP*, pages 507–520. Springer, 2008.

[35] J. Rathke and P. Sobocinski. Deriving structural labelled transitions for mobile ambients. In *CONCUR '08*, volume 5201 of *LNCS*, pages 462–476. Springer, 2008.

[36] D. Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis, Department of Computer Science, University of Edinburgh, 1992.

[37] D. Sangiorgi. Bisimulation for higher-order process calculi. *Information and Computation*, 131(2):141–178, 1996.

[38] D. Sangiorgi, N. Kobayashi, and E. Sumii. Environmental bisimulations for higher-order languages. In *LICS '07*, pages 293–302. IEEE Computer Society, 2007.

[39] D. Sangiorgi and D. Walker. *The Pi-Calculus: A Theory of Mobile Processes*. Cambridge University Press, 2001.

[40] A. Schmitt and J.-B. Stefani. The M-calculus: A higher-order distributed process calculus. In *POPL'03*, pages 50–61, New Orleans, LA, USA, January 2003.

[41] A. Schmitt and J.-B. Stefani. The Kell Calculus: A Family of Higher-Order Distributed Process Calculi. In *Global Computing 2004 workshop*, volume 3267 of *LNCS*, 2004.

[42] P. Sewell, J. Leifer, K. Wansbrough, F. Zappa Nardelli, M. Allen-Willians, P. Habouzit, and V. Vafeiadis. Acute: High-level programming language design for distributed computation. *Journal of Functional Programming*, 17(4-5), 2007.

[43] B. Thomsen. Plain chocs: A second generation calculus for higher order processes. *Acta Informatica*, 30(1):1–59, 1993.

[44] P. Wojciechowski and P. Sewell. Nomadic Pict: Language and Infrastructure. *IEEE Concurrency, vol. 8, no 2*, 2000.

[45] A. Ziegler, D. Miller, and C. Palamidessi. A congruence format for name-passing calculi. *Electr. Notes Theor. Comput. Sci.*, 156(1):169–189, 2006.

Appendix A. Weak Complementary Semantics in HOπP

In this section, we first prove the relation between the context and complementary LTS and bisimilarities (Theorem 9). We then prove soundness (Theorem 8) and completeness (Theorem 10) of the weak complementary bisimilarity with respect to barbed congruence.

Appendix A.1. Correspondence Lemmas

Lemma 15. *If $P \xrightarrow{a} F$, then for all R we have $P \xmapsto{a,R} F \circ R$. If $P \xmapsto{a,R} P'$, then there exists F such that $P \xrightarrow{a} F$ and $P' = F \circ R$.*

Proof. We proceed by structural induction on P.

- If $P = a(X)P'$, then by rule Abstr we have $P \xrightarrow{a} F = (X)P'$, and by rule In_i^p we have $P \xmapsto{a,R} P'\{R/X\} = F \circ R$ for all R, hence the result holds.
- Let $P = P_1 \mid P_2$. Suppose we have $P \xrightarrow{a} F$, which is possible only by rule Par (and its symmetric, which is handled similarly). Consequently we have $P_1 \xrightarrow{a} F'$ and $F = F' \mid P_2$. By induction we have $P_1 \xmapsto{a,R} F' \circ R$ for all R, hence by rule $\text{Par}_{i\tau}^p$ we have $P \xmapsto{a,R} F' \circ R \mid P_2 = F \circ R$, as required. Suppose we have $P \xmapsto{a,R} P'$, which is possible only by rule $\text{Par}_{i\tau}^p$ (and its symmetric, which is handled similarly). Consequently we have $P_1 \xmapsto{a,R} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists F such that $P_1 \xrightarrow{a} F$ and $P_1' = F \circ R$. Consequently by rule Par we have $P \xrightarrow{a} F \mid P_2$ with $P' = (F \mid P_2) \circ R$, as required.
- The locality, restriction, and replication cases are similar to the parallel case.

□

For a concretion $C = \nu\widetilde{b}.\langle R\rangle S$, we remind that $extr(C) \triangleq \text{fn}(R) \setminus \widetilde{b}$.

Lemma 16. *Let P be an HOπP process.*

Suppose $P \xrightarrow{\overline{a}} C$. For all Q such that $Q \xrightarrow{a} F$ and for all $\mathbb{E}$ such that $nbh(\mathbb{E}) \cap extr(C) = \emptyset$, we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{extr(C)} F \bullet \mathbb{E}\{C\}$.

If $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, then there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = extr(C)$, and $P' = F \bullet \mathbb{E}\{C\}$.

Proof. We proceed by structural induction induction on P.

- Let $P = \overline{a}\langle P_1\rangle P_2$. We have $P \xrightarrow{\overline{a}} \langle P_1\rangle P_2 = C$. Let Q such that $Q \xrightarrow{a} F$ and $\mathbb{E}$ such that $\mathrm{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$. We have $F \bullet \mathbb{E}\{C\} = F \circ P_1 \mid \mathbb{E}\{P_2\}$. By Lemma 15, we have $Q \xmapsto{a,P_1} F \circ P_1$. Let $\widetilde{b} = \mathrm{fn}(P_1)$; by rule $\textsc{Out}^p_o$, we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$ with $\widetilde{b} = \mathrm{fn}(P_1) = extr(C)$ as wished.

  We now prove the reverse implication. We have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} Q' \mid \mathbb{E}\{P_2\}$ with $Q \xmapsto{a,P_1} Q'$ and $\widetilde{b} = \mathrm{fn}(P_1)$. By Lemma 15, there exists F such that $Q \xrightarrow{a} F$ and $Q' = F \circ P_1$. Let $C = \langle P_1\rangle P_2$. We have $P \xrightarrow{\overline{a}} C$, $P' = F \bullet \mathbb{E}\{C\}$ and $\widetilde{b} = \mathrm{fn}(P_1) = extr(C)$, as required.

- Let $P = P_1 \mid P_2$. Suppose we have $P \xrightarrow{\overline{a}} C$, which is possible by rule $\textsc{Par}$ or its symmetric. In the case of rule $\textsc{Par}$, we have $P_1 \xrightarrow{a} C'$ and $C = C' \mid P_2$. Let $Q \xrightarrow{a} F$ and $\mathbb{E}$ be an evaluation context. By induction we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\Box \mid P_2\}}_{\widetilde{b}} F \bullet \mathbb{E}\{C' \mid P_2\}$ with $\widetilde{b} = extr(C')$. By rule $\textsc{Par}^p_o$ we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$, and we have $\widetilde{b} = extr(C') = extr(C)$, as required.

  Suppose we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, which is possible by rule $\textsc{Par}^p_o$ or its symmetric. In the case of rule $\textsc{Par}^p_o$, we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\Box \mid P_2\}}_{\widetilde{b}} P'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = extr(C)$ and $P' = F \bullet \mathbb{E}\{C \mid P_2\}$. Consequently by rule $\textsc{Par}$ we have $P \xrightarrow{\overline{a}} C \mid P_2 = C'$ with $P' = F \bullet \mathbb{E}\{C'\}$ and $\widetilde{b} = extr(C) = extr(C')$, as required.

- The locality case is similar to the parallel one for the evaluation rules ($\textsc{Loc}$ and $\textsc{Loc}^p_o$), and to the message output one for the passivation rules ($\textsc{Passiv}$ and $\textsc{Passiv}^p_o$).

- The replication case is similar to the parallel one.

- Let $P = \nu c.P_1$. Suppose first we have $P \xrightarrow{\overline{a}} C$. By rule $\textsc{Restr}$ we have $P_1 \xrightarrow{\overline{a}} C'$ and $C = \nu c.C'$. Let $Q \xrightarrow{a} F$ and $\mathbb{E}$ be an evaluation context. We distinguish two cases:
  - If $c \in extr(C')$, then we have $F \bullet \mathbb{E}\{\nu c.C'\} = \nu c.(F \bullet \mathbb{E}\{C'\})$. By induction we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'_1$ with $\widetilde{b} = extr(C')$ and $P'_1 = F \bullet \mathbb{E}\{C'\}$. We have $c \in \widetilde{b}$, so by rule $\textsc{Extr}^p_o$ we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}\setminus\{c\}} \nu c.P'_1 = F \bullet \mathbb{E}\{\nu c.C'\}$. We have $extr(C) = extr(C') \cup \{c\}) = \widetilde{b} \setminus \{c\}$, hence the result holds.
  - If $c \notin extr(C')$, then by induction we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu b.\Box\}}_{\widetilde{b}} P'_1$ with $\widetilde{b} = extr(C')$ and $P'_1 = F \bullet \mathbb{E}\{\nu c.C'\} = F \bullet \mathbb{E}\{C\}$. By rule $\textsc{Restr}^p_o$

we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$, and we have $\widetilde{b} = extr(C') = extr(C)$, as required.

Suppose now that $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$. We have two cases:

- Rule $\textsc{Restr}^p_o$: we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}_{\widetilde{b}} P'$ with $c \notin \widetilde{b}$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = extr(C)$ and $P' = F \bullet \mathbb{E}\{\nu c.C\}$. By rule $\textsc{Restr}$ we have $P \xrightarrow{\overline{a}} \nu c.C = C'$, and $extr(C') = extr(C) = \widetilde{b}$ since $c \notin \widetilde{b}$. We have $P' = F \bullet \mathbb{E}\{C'\}$, as required.
- Rule $\textsc{Extr}^p_o$: we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}\cup\{c\}} P'_1$ with $P' = \nu c.P'_1$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} \cup \{c\} = extr(C)$, and $P'_1 = F \bullet \mathbb{E}\{C\}$. By rule $\textsc{Restr}$ we have $P \xrightarrow{\overline{a}} \nu c.C = C'$. Since $\widetilde{b} \cup \{c\} = extr(C)$, c is free in the message of C, consequently we have $F \bullet \mathbb{E}\{C'\} = \nu c.(F \bullet \mathbb{E}\{C\}) = P'$[6]. We also have $\widetilde{b} = extr(C) = extr(C')$, as required.

□

Lemma 17. *Let P be an HOπP process.*

If $P \xrightarrow{\overline{a}} C$, then for all Q such that $Q \xrightarrow{a} F$ and for all $\mathbb{E}$, we have $P \xmapsto{\overline{a},Q,\mathbb{E}}_{extr(C)} F \bullet \mathbb{E}\{C\}$.

If $P \xmapsto{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, then there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = extr(C)$, and $P' = F \bullet \mathbb{E}\{C\}$.

Proof. Let $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, and $\mathbb{E}$ an evaluation context. We prove the first result by induction on the number of captures by $\mathbb{E}$, i.e. on the size of the set $\text{nbh}(\mathbb{E}) \cap extr(C)$. If $\text{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$, then by Lemma 16 we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{extr(C)} F \bullet \mathbb{E}\{C\}$. By rule $\textsc{CFree}^p_o$ we have the required result.

Otherwise, there exists $c, \mathbb{E}_1\mathbb{E}_2$ such that $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$. The context $\mathbb{E}_1\{\mathbb{E}_2\}$ is performing less capture than $\mathbb{E}$, so by induction we have $P \xmapsto{\overline{a},Q,\mathbb{E}_1\{\mathbb{E}_2\}}_{extr(C)} F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}$. By rule $\textsc{Capt}^p_o$, we have $P \xmapsto{\overline{a},Q,\mathbb{E}}_{extr(C)} \nu c.(F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}) = F \bullet \mathbb{E}\{C\}$, as required.

We prove the reverse implication by induction on the derivation of $P \xmapsto{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$. If the transition comes from rule $\textsc{CFree}^p_o$, we have $\text{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$, and we can use Lemma 16. Otherwise, by rule $\textsc{Capt}^p_o$ there exists $c, \mathbb{E}_1, \mathbb{E}_2, P''$ such that $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, $P \xmapsto{\overline{a},Q,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}} P''$ with $P' = \nu c.P''$, and $c \in \widetilde{b}$. By

[6]Note that, because c is bound in P, c is not free in Q and $\mathbb{E}$ by our convention on bound names, so no unintended capture happens there

induction there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $P'' = F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}$, and $extr(C) = \widetilde{b}$. Since $c \in \widetilde{b} = extr(C)$, we have $F \bullet \mathbb{E}\{C\} = \nu c.(F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}) = \nu c.P'' = P'$, as required.

□

Lemma 18. *Let P be an HOπP process. We have $P \xrightarrow{\tau} P'$ iff $P \overset{\tau}{\longmapsto} P'$.*

Proof. We proceed by structural induction on P.

Let $P = P_1 \mid P_2$. By case analysis on the rule used to derive $P \xrightarrow{\tau} P'$:

- PAR: in this case we have $P_1 \xrightarrow{\tau} P_1'$ and $P' = P_1' \mid P_2$. By induction we have $P_1 \overset{\tau}{\longmapsto} P_1'$, hence by rule $\text{PAR}^p_{i\tau}$ we have $P \overset{\tau}{\longmapsto} P'$, as required.
- HO: in this case, we have $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\overline{a}} C$, and $P' = F \bullet C$. By induction we have $P_2 \xmapsto{\overline{a}, P_1, \square}_{\widetilde{b}} F \bullet C$, so by rule HO^p_τ we have $P \overset{\tau}{\longmapsto} P'$, as required.

We now prove the reverse implication.

- $\text{PAR}^p_{i\tau}$: we have $P_1 \overset{\tau}{\longmapsto} P_1'$ and $P' = P_1' \mid P_2$. By induction we have $P_1 \xrightarrow{\tau} P_1'$, hence we have $P \xrightarrow{\tau} P_1' \mid P_2$ by rule PAR.
- HO^p_τ: we have $P_1 \xmapsto{\overline{a}, P_2, \square}_{\widetilde{b}} P'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $P_2 \xrightarrow{a} F$ and $P' = F \bullet C$. By rule HO, we have $P \xrightarrow{\tau} P'$, as required.

The locality, restriction, and replication cases are similar.

□

Lemma 19. *Let P be an HOπP process.*

- *We have $P \overset{\tau}{\Rightarrow} P'$ iff $P \overset{\tau}{\Mapsto} P'$.*
- *Let R be a closed process. If $P \overset{a}{\Rightarrow} F$ and $F \circ R \overset{\tau}{\Rightarrow} P'$ then we have $P \overset{a,R}{\Longmapsto} F \circ R$. If $P \overset{a,R}{\Longmapsto} P'$, then there exists F such that $P \overset{a}{\Rightarrow} F$ and $F \circ R \overset{\tau}{\Rightarrow} P'$.*
- *If $P \overset{\overline{a}}{\Rightarrow} C$, then for all $Q, \mathbb{E}$ such that $Q \overset{a}{\Rightarrow} F$ and $F \bullet \mathbb{E}\{C\} \overset{\tau}{\Rightarrow} P'$, we have $P \xmapsto{\overline{a}, Q, \mathbb{E}}_{\widetilde{b}} P'$ with $\widetilde{b} = extr(C)$. If $P \xmapsto{\overline{a}, Q, \mathbb{E}}_{\widetilde{b}} P'$, then there exists F, C such that $P \overset{\overline{a}}{\Rightarrow} C$, $Q \overset{a}{\Rightarrow} F$, $\widetilde{b} = extr(C)$, and $F \bullet \mathbb{E}\{C\} \overset{\tau}{\Rightarrow} P'$.*

Proof. By Lemma 18 we have $\xrightarrow{\tau} = \overset{\tau}{\longmapsto}$, so we have $\overset{\tau}{\Rightarrow} = \overset{\tau}{\Mapsto}$.

If $P \overset{\tau}{\Rightarrow} P'' \xrightarrow{a} F$ and $F \circ R \overset{\tau}{\Rightarrow} P'$, then we have $P \overset{\tau}{\Mapsto} P''$ and $F \circ R \overset{\tau}{\Mapsto} P'$ by the first result. By Lemma 15 we have $P'' \xmapsto{a,R} F \circ R$, consequently we have $P \overset{a,R}{\Longmapsto} P'$. If $P \overset{\tau}{\Mapsto} P_1 \xmapsto{a,R} P_2 \overset{\tau}{\Mapsto} P'$, then we have $P \overset{\tau}{\Rightarrow} P_1$ and $P_2 \overset{\tau}{\Rightarrow} P'$. By Lemma 15 there exists F such that $P_1 \xrightarrow{a} F$ and $F \circ R = P_2$. Consequently we have $P \overset{a}{\Rightarrow} F$ and $F \circ R \overset{\tau}{\Rightarrow} P'$ as wished.

Let $P \stackrel{\tau}{\Rightarrow} P'' \stackrel{\overline{a}}{\rightarrow} C$, $Q \stackrel{\tau}{\Rightarrow} Q'' \stackrel{a}{\rightarrow} F$, and $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$. We have $P \stackrel{\tau}{\Rightarrow} P''$, $Q \stackrel{\tau}{\Rightarrow} Q''$ and $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$ by the first result. By Lemma 17 we have $P'' \stackrel{\overline{a},Q'',\mathbb{E}}{\longmapsto_{\widetilde{b}}} F \bullet \mathbb{E}\{C\}$ with $\widetilde{b} = extr(C)$, so we have $P \stackrel{\overline{a},Q'',\mathbb{E}}{\Longmapsto_{\widetilde{b}}} P'$. Consequently we have $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto_{\widetilde{b}}} P'$, as required. If $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto_{\widetilde{b}}} P'$, then we have $P \stackrel{\tau}{\Rightarrow} P_1 \stackrel{\overline{a},Q',\mathbb{E}}{\longmapsto_{\widetilde{b}}} P_2 \stackrel{\tau}{\Rightarrow} P'$ with $Q \stackrel{\tau}{\Rightarrow} Q'$. We have $P \stackrel{\tau}{\Rightarrow} P_1$, $P_2 \stackrel{\tau}{\Rightarrow} P'$, and $Q \stackrel{\tau}{\Rightarrow} Q'$ by the first result. By Lemma 17 there exists F, C such that $P_1 \stackrel{\overline{a}}{\rightarrow} C$, $Q' \stackrel{a}{\rightarrow} F$, $\widetilde{b} = extr(C)$, and $P_2 = F \bullet \mathbb{E}\{C\}$. Consequently we have $P \stackrel{\overline{a}}{\Rightarrow} C$, $Q \stackrel{a}{\Rightarrow} F$, and $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$, as required. □

We now prove the correspondence between $\approx$ and $\approx_m$. The correspondence proof for $\sim$ and $\sim_m$ is similar.

Lemma 20. *If $P \stackrel{\overline{a}}{\rightarrow} C$ then we have $fn(C) \subseteq fn(P)$.*

Proof. By induction on $P \stackrel{\overline{a}}{\rightarrow} C$. □

Lemma 21. *Let $P \approx Q$. Let $P \stackrel{\overline{a}}{\rightarrow} C$, F an abstraction, and $Q \stackrel{\overline{a}}{\Rightarrow} C'$ such that for all $\mathbb{E}$, there exists Q' such that $F \bullet \mathbb{E}\{C'\} \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet \mathbb{E}\{C\} \approx Q'$. Then we have $extr(C) = extr(C')$.*

Proof. Similar to the one of Lemma 8. □

Theorem 16 (**Theorem 9**). *If $P \approx Q$ then $P \approx_m Q$.*

Proof. We prove that $\approx$ is a weak complementary bisimulation. Let $P \approx Q$. We have $\mathrm{fn}(P) = \mathrm{fn}(Q)$ by definition.

- If $P \stackrel{\tau}{\longmapsto} P'$ then by Lemma 18 we have $P \stackrel{\tau}{\rightarrow} P'$. By definition there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx Q'$. By Lemma 19 we have $Q \stackrel{\tau}{\Rightarrow} Q'$, and we have $P' \approx Q'$ as wished.

- If $P \stackrel{a,R}{\longmapsto} P'$, then by Lemma 15 there exists F such that $P \stackrel{a}{\rightarrow} F$ and $P' = F \circ R$. By definition there exists G, Q' such that $Q \stackrel{a}{\Rightarrow} G$, $G \bullet \langle R \rangle \mathbf{0} \stackrel{\tau}{\Rightarrow} Q'$ and $Q' \approx F \bullet \langle R \rangle \mathbf{0}$. We have $G \bullet \langle R \rangle \mathbf{0} \equiv G \circ R$ so by Lemma 19 we have $Q \stackrel{a,R}{\Longmapsto} Q' \approx F \bullet \langle R \rangle \mathbf{0} \equiv P'$ as wished.

- If $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$, then by Lemma 17 there exists F, C such that $T \stackrel{a}{\rightarrow} F$, $P \stackrel{\overline{a}}{\rightarrow} C$, $\widetilde{b} = extr(C)$ and $P' = F \bullet \mathbb{E}\{C\}$. By definition there exists D, Q' such that $Q \stackrel{\overline{a}}{\Rightarrow} D$, $F \bullet \mathbb{E}\{D\} \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet \mathbb{E}\{C\} \approx Q'$. By Lemma 21 we have $extr(D) = extr(C) = \widetilde{b}$. By Lemma 19 we have $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto_{\widetilde{b}}} Q'$, and we have $P' \approx Q'$ as required.

□

Appendix A.2. Howe's Method

We now prove the soundness of $\approx_m$ using Howe's method. We remind that $\overset{\lambda}{\mapsto}$ ranges over $\overset{\tau}{\mapsto}$, $\overset{a,R}{\longmapsto}$, and $\overset{\overline{a},Q,\mathbb{E}}{\longmapsto_{\widetilde{b}}}$, and $\overset{\lambda}{\Rightarrow}$ ranges over the weak transitions.

Lemma 22. *If $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$, then $nbh(\mathbb{E}) \cap \widetilde{b} = \emptyset$.*

Proof. Easy by induction on $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$. □

Lemma 23. *If $P \approx_m Q$ and $P \overset{\overline{a},T,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$, then there exists T', Q' such that $T \overset{\tau}{\Rightarrow} T'$, $Q \overset{\tau}{\Rightarrow} \overset{\overline{a},T',\mathbb{E}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Rightarrow} Q'$, and $P' \approx_m Q'$.*

Proof. Since we have $P \overset{\overline{a},T,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$, we have $P \overset{\overline{a},T,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$ by rule CFREE_o^p, and we have $\text{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$ by Lemma 22. By bisimilarity, there exists Q' such that $Q \overset{\overline{a},T,\mathbb{E}}{\Longmapsto_{\widetilde{b}}} Q'$, and $P' \approx_m Q'$. By definition there exists T' such that $Q \overset{\tau}{\Rightarrow} \overset{\overline{a},T',\mathbb{E}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Rightarrow} Q'$. Because $\text{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$, context $\mathbb{E}$ is capture-free w.r.t. to $\widetilde{b}$, so the output transition comes from rule CFREE_o^p. Consequently we have $Q \overset{\tau}{\Rightarrow} \overset{\overline{a},T',\mathbb{E}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Rightarrow} Q'$ as wished.

□

Lemma 24. *Let $P \approx_m Q$*

- *If $P \overset{\lambda}{\Rightarrow} P'$ then there exists Q' such that $Q \overset{\lambda}{\Rightarrow} Q'$ and $P' \approx_m Q'$.*
- *If there exists T' such that $T \overset{\tau}{\Rightarrow} T'$ and $P \overset{\tau}{\Rightarrow} \overset{\overline{a},T',\mathbb{E}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Rightarrow} P'$, then there exists T'', Q' such that $T \overset{\tau}{\Rightarrow} T''$, $Q \overset{\tau}{\Rightarrow} \overset{\overline{a},T'',\mathbb{E}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Rightarrow} Q'$, and $P' \approx_m Q'$*

Proof. If $P \overset{\tau}{\Rightarrow} P'$, we proceed by induction on the number of τ-steps. For 0 step, the result holds (chose $Q' = Q$). Suppose the result holds for n. If $P(\overset{\tau}{\mapsto})^n P_n \overset{\tau}{\mapsto} P'$, then by induction there exists Q'_n such that $Q \overset{\tau}{\Rightarrow} Q'_n$ and $P'_n \approx_m Q'_n$. By bisimulation definition, there exists Q' such that $Q'_n \overset{\tau}{\Rightarrow} Q'$ and $P' \approx_m Q'$. Since we have $Q \overset{\tau}{\Rightarrow} Q'$, we have the required result.

If $P \overset{\tau}{\Rightarrow} P_1 \overset{a,R}{\longmapsto} P_2 \overset{\tau}{\Rightarrow} P'$, then by the first result there exists Q'_1 such that $Q \overset{\tau}{\Rightarrow} Q'_1$ and $P_1 \approx_m Q'_1$. By bisimulation definition there exists Q'_2 such that $P \overset{a,R}{\Longmapsto} Q'_2$ and $P_2 \approx_m Q'_2$. By the first result there exists $Q'_2 \overset{\tau}{\Rightarrow} Q'$ and $P' \approx_m Q'$. We have $Q \overset{a,R}{\Longmapsto} Q'$ hence the result holds.

If $P \overset{\tau}{\Rightarrow} P_1 \overset{\overline{a},T',\mathbb{E}}{\longmapsto_{\widetilde{b}}} P_2 \overset{\tau}{\Rightarrow} P'$ with $T \overset{\tau}{\Rightarrow} T'$, then by the first result there exists Q'_1 such that $Q \overset{\tau}{\Rightarrow} Q'_1$ and $P_1 \approx_m Q'_1$. By bisimulation definition there exists Q'_2 such that $Q'_1 \overset{\overline{a},T',\mathbb{E}}{\Longmapsto_{\widetilde{b}}} Q'_2$ and $P_2 \approx Q'_2$. By the first result there exists

Q' such that $Q'_2 \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx_m Q'$. We have $Q \stackrel{\overline{a},T,\mathbb{E}}{\overset{\cdots}{\longmapsto}}_{\widetilde{b}} Q'$ as wished.

If $P \stackrel{\tau}{\Rightarrow} P_1 \stackrel{\overline{a},T',\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P_2 \stackrel{\tau}{\Rightarrow} P'$ with $T \stackrel{\tau}{\Rightarrow} T'$, then by the first result there exists Q'_1 such that $Q \stackrel{\tau}{\Rightarrow} Q'_1$ and $P_1 \approx_m Q'_1$. By Lemma 23 there exists T'', Q'_2 such that $T' \stackrel{\tau}{\Rightarrow} T''$, $Q'_1 \stackrel{\tau}{\Rightarrow} \stackrel{\overline{a},T'',\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'_2$ and $P_2 \approx Q'_2$. By the first result there exists Q' such that $Q'_2 \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx_m Q'$. We have $Q \stackrel{\tau}{\Rightarrow} \stackrel{\overline{a},T'',\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$ with $T \stackrel{\tau}{\Rightarrow} T''$, as wished.

□

We recall the definitions of open extension and Howe's closure of weak bisimilarity $\approx_m$.

Definition 21. *Let P and Q be two open processes. We have $P \approx^\circ_m Q$ iff $P\sigma \approx_m Q\sigma$ for all substitutions that close P and Q.*

Definition 22. *The Howe's closure $\approx^\bullet_m$ is the smallest relation verifying:*

- $\approx^\circ_m \subseteq \approx^\bullet_m$.
- $\approx^\bullet_m \approx^\circ_m \subseteq \approx^\bullet_m$.
- *For all operators op of the language, if $\widetilde{P} \approx^\bullet_m \widetilde{Q}$, then $op(\widetilde{P}) \approx^\bullet_m op(\widetilde{Q})$.*

Lemma 25. *$\approx^\bullet_m$ is reflexive.*

Proof. Because $\approx_m$ is reflexive. □

Lemma 26. *If $P \approx^\bullet_m Q$, then $fn(P) = fn(Q)$.*

Proof. By induction on the derivation of $P \approx^\bullet_m Q$.

- If $P \approx_m Q$, then we have $\mathrm{fn}(P) = \mathrm{fn}(Q)$ by definition.
- If $P \approx^\bullet_m T \approx_m Q$, then we have $\mathrm{fn}(P) = \mathrm{fn}(T)$ by induction, and $\mathrm{fn}(T) = \mathrm{fn}(Q)$ by bisimulation definition. Consequently we have $\mathrm{fn}(P) = \mathrm{fn}(Q)$.
- If $\widetilde{P} \approx^\bullet_m \widetilde{Q}$, we have $\mathrm{fn}(P_i) = \mathrm{fn}(Q_i)$ for each item on the list by induction, hence using definition of free names we have $\mathrm{fn}(op(\widetilde{P})) = \mathrm{fn}(op(\widetilde{Q}))$.

□

Lemma 27. *If $R \approx^\bullet_m R'$, then $P\{R/X\} \approx^\bullet_m P\{R'/X\}$.*

If $P \stackrel{a,R}{\longmapsto} P'$ and $R \approx^\bullet_m R'$, then there exists P'' such that $P \stackrel{a,R'}{\longmapsto} P''$ and $P' \approx^\bullet_m P''$.

Proof. The first item is done by structural induction on P:

- $P = \mathbf{0}$: the result holds.
- $P = X$: $P\{R/X\} = R \approx^\bullet_m R' = P\{R'/X\}$, hence the result holds.

- $P = Y \neq X$: the result holds.
- $P = P_1 \mid P_2$: by induction $P_1\{R/X\} \approx^{\bullet}_m P_1\{R'/X\}$ and $P_2\{R/X\} \approx^{\bullet}_m P_2\{R'/X\}$ hold. Since $\approx^{\bullet}_m$ is a congruence we have $P\{R/X\} = P_1\{R/X\} \mid P_2\{R/X\} \approx^{\bullet}_m P_1\{R'/X\} \mid P_2\{R'/X\} = P\{R'/X\}$, as required.
- The locality, message input, message output, and replication cases are similar to the case above.
- $P = \nu a.P_1$. By induction we have $P_1\{R/X\} \approx^{\bullet}_m P_1\{R'/X\}$. Since $\approx^{\bullet}_m$ is a congruence, we have $P\{R/X\} = \nu a.(P_1\{R/X\}) \approx^{\bullet}_m \nu a.(P_1\{R'/X\}) = P\{R'/X\}$, as required.

The second item is proved by induction on the derivation of $P \overset{a,R}{\longmapsto} P'$:

- Rule $\textsc{In}^p_i$: we have $P = a(X)P_1 \overset{a,R}{\longmapsto} P_1\{R/X\}$. Using first item we have $P_1\{R/X\} \approx^{\bullet}_m P_1\{R'/X\}$, and by rule $\textsc{In}^p_i$ we have $P \overset{a,R'}{\longmapsto} P_1\{R'/X\}$, as required.
- Rule $\textsc{Par}^p_{i\tau}$: we have $P = P_1 \mid P_2$ with $P_1 \overset{a,R}{\longmapsto} P'_1$ and $P' = P'_1 \mid P_2$. By induction there exists P''_1 such that $P_1 \overset{a,R'}{\longmapsto} P''_1$ and $P'_1 \approx^{\bullet}_m P''_1$. By rule $\textsc{Par}^p_{i\tau}$, we have $P \overset{a,R'}{\longmapsto} P''_1 \mid P_2 = P''$, and since $\approx^{\bullet}_m$ is a congruence, we have $P' \approx^{\bullet}_m P''$, as required.
- Rules $\textsc{Loc}^p_{i\tau}$ and $\textsc{Replic}^p_{i\tau}$: similar to the case above.
- Rule $\textsc{Restr}^p_{i\tau}$: we have $P = \nu b.P_1$ with $P_1 \overset{a,R}{\longmapsto} P'_1$, $b \neq a$, and $P' = \nu b.P'_1$. By induction there exists P''_1 such that $P_1 \overset{a,R'}{\longmapsto} P''_1$ and $P'_1 \approx^{\bullet}_m P''_1$. By rule $\textsc{Restr}^p_{i\tau}$ we have $P \overset{a,R}{\longmapsto} \nu b.P''_1 = P''$, and since $\approx^{\bullet}_m$ is a congruence we have $P' \approx^{\bullet}_m P''$, as required.

□

Lemma 28. *For all $P \approx^{\bullet}_m Q$ and all $R \approx^{\bullet}_m R'$, we have $P\{R/X\} \approx^{\bullet}_m Q\{R'/X\}$.*

Proof. By induction on the derivation of $P \approx^{\bullet}_m Q$.

- $P \approx^{\circ}_m Q$: by Lemma 27, we have $P\{R/X\} \approx^{\bullet}_m P\{R'/X\}$. Let σ be a substitution which closes R' and P, Q except for X. By open extension definition we have $P\{R'\sigma/X\}\sigma \approx_m Q\{R'\sigma/X\}\sigma$, i.e. we have $P\{R'/X\}\sigma \approx_m Q\{R'/X\}$. Consequently we have $P\{R'/X\} \approx^{\circ}_m Q\{R'/X\}$, so we have $P\{R/X\} \approx^{\bullet}_m \approx^{\circ}_m Q\{R'/X\}$, i.e. $P\{R/X\} \approx^{\bullet}_m Q\{R'/X\}$, as required.
- $P \approx^{\bullet}_m T \approx^{\circ}_m Q$: by induction we have $P\{R/X\} \approx^{\bullet}_m T\{R'/X\}$, and using the same technique as in the first case we have $T\{R'/X\} \approx^{\circ}_m Q\{R'/X\}$, hence we have $P\{R/X\} \approx^{\bullet}_m Q\{R'/X\}$, as required.

- $op(\widetilde{P'}) \approx^{\bullet}_m op(\widetilde{Q'})$ with $\widetilde{P'} \approx^{\bullet}_m \widetilde{Q'}$. By induction we have $\widetilde{P'\{R/X\}} \approx^{\bullet}_m \widetilde{Q'\{R'/X\}}$, hence we have $op(\widetilde{P'\{R/X\}}) \approx^{\bullet}_m op(\widetilde{Q'\{R'/X\}})$ since $\approx^{\bullet}_m$ is congruence. Consequently we have $P\{R/X\} \approx^{\bullet}_m Q\{R'/X\}$, as required.

□

We write $(\approx_m)^{\bullet}_c$ the restriction of $\approx^{\bullet}_m$ to closed processes.

Lemma 29. *Let $P \approx^{\bullet}_m Q$. For every substitution σ, we have $P\sigma \approx^{\bullet}_m Q\sigma$ using a derivation of the same size.*

Proof. By induction on $P \approx^{\bullet}_m Q$. Most cases are immediate by induction. The base case is $P \approx^{\circ}_m Q$. We show that $P\sigma \approx^{\circ}_m Q\sigma$. Let σ' a substitution that closes $P\sigma$ and $Q\sigma$, then $\sigma\sigma'$ closes P and Q, thus $P\sigma\sigma' \approx_m Q\sigma\sigma'$.

□

Lemma 30. *Let $P\ (\approx_m)^{\bullet}_c\ Q$. If $P \xmapsto{a,R} P'$, then for all R' such that $R\ (\approx_m)^{\bullet}_c\ R'$, there exists Q' such that $Q \xRightarrow{a,R} Q'$ and $P'\ (\approx_m)^{\bullet}_c\ Q'$.*

Proof. By induction on the size of the derivation of $P\ (\approx_m)^{\bullet}_c\ Q$.

- $P \approx^{\circ}_m Q$. Since P, R are closed, P' is closed. By Lemma 27 there exists P'' such that $P \xmapsto{a,R'} P''$ and $P' \approx^{\bullet}_m P''$. Since P, Q are closed, we have $P \approx_m Q$; by bisimulation definition there exists Q' such that $Q \xRightarrow{a,R'} Q'$ and $P'' \approx_m Q'$. Let σ be a substitution that closes P''. Since Q, R' are closed, Q' is closed and we have $P''\sigma \approx_m Q'$ by Lemma 28. Consequently, we have $P' \approx^{\bullet}_m \approx^{\circ}_m Q'$, and since P', Q' are closed, we have $P'\ (\approx_m)^{\bullet}_c\ Q'$, as required.

- $P \approx^{\bullet}_m T \approx^{\circ}_m Q$. Let σ be a substitution that closes T; since P is closed and by lemma 29, we have $P \approx^{\bullet}_m T\sigma$. By induction there exists T' such that $T\sigma \xRightarrow{a,R'} T'$ and $P'\ (\approx_m)^{\bullet}_c\ T'$. By open extension definition and since Q is closed, we have $T\sigma \approx_m Q$. By Lemma 24 there exists Q' such that $Q \xRightarrow{a,R'} Q'$ and $T' \approx^{\bullet}_m Q'$. Consequently we have $P' \approx^{\bullet}_m \approx^{\circ}_m Q'$, and since P, Q, R, R' are closed, P', Q' are closed too. Finally we have $P'\ (\approx_m)^{\bullet}_c\ Q'$ as required.

- $op(\widetilde{P}) \approx^{\bullet}_m op(\widetilde{Q})$ with $\widetilde{P} \approx^{\bullet}_m \widetilde{Q}$. By case analysis on op.

  - $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$ with $P_1 \xmapsto{a,R} P'_1$. By induction there exists Q'_1 such that $Q_1 \xRightarrow{a,R'} Q'_1$ and $P'_1 \approx^{\bullet}_m Q'_1$. Using rules $\textsc{Par}^{p}_{i\tau}$ for τ-actions and $\textsc{Par}^{p}_{i\tau}$ for the observable action, we have $Q \xRightarrow{a,R'} Q'_1 \mid Q_2$. Since $\approx^{\bullet}_m$ is a congruence, we have $P'_1 \mid P_2 \approx^{\bullet}_m Q'_1 \mid Q_2$. Since P, Q, R, R' are closed, all the involved processes are closed and we have $P'_1 \mid P_2\ (\approx_m)^{\bullet}_c\ Q'_1 \mid Q_2$, as required.
  - Locality, replication: similar to the case above.

– $P = a(X)P_1$, $Q = a(X)Q_1$ with $P \xmapsto{a,R} P_1\{R/X\}$. By Lemma 28, we have $P_1\{R/X\} \approx^{\bullet}_m Q_1\{R'/X\}$. Using rule IN^p_i, we have $Q \xmapsto{a,R'} Q_1\{R'/X\}$. Since the involved processes are closed, we have $P_1\{R/X\}\ (\approx_m)^{\bullet}_c\ Q_1\{R/X\}$ as required.
– $P = \nu b.P_1$ and $Q = \nu b.Q_1$. Similar to the parallel case.

□

We inductively define $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ as:

- $\Box \approx^{\bullet}_m \Box$
- If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ and $P \approx^{\bullet}_m Q$ then $\mathbb{E} \mid P \approx^{\bullet}_m \mathbb{F} \mid Q$ and $P \mid \mathbb{E} \approx^{\bullet}_m Q \mid \mathbb{F}$.
- If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ then $\nu a.\mathbb{E} \approx^{\bullet}_m \nu a.\mathbb{F}$.
- If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ then $a[\mathbb{E}] \approx^{\bullet}_m a[\mathbb{F}]$.

Lemma 31. *If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$, $P \approx^{\bullet}_m Q$, and $\mathbb{E}' \approx^{\bullet}_m \mathbb{F}'$ then $\mathbb{E}\{P\} \approx^{\bullet}_m \mathbb{F}\{Q\}$ and $\mathbb{E}\{\mathbb{E}'\} \approx^{\bullet}_m \mathbb{F}\{\mathbb{F}'\}$.*

Proof. By induction on $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$.

- $\Box \approx^{\bullet}_m \Box$: the result holds.
- $\mathbb{E}_1 \mid P_1 \approx^{\bullet}_m \mathbb{F}_1 \mid Q_1$ by induction we have $\mathbb{E}_1\{P\} \approx^{\bullet}_m \mathbb{F}_1\{Q\}$ and $\mathbb{E}_1\{\mathbb{E}'\} \approx^{\bullet}_m \mathbb{F}_1\{\mathbb{F}'\}$. By congruence we have $\mathbb{E}_1\{P\} \mid P_1 \approx^{\bullet}_m \mathbb{F}_1\{Q\} \mid Q_1$ and $\mathbb{E}_1\{\mathbb{E}'\} \mid P_1 \approx^{\bullet}_m \mathbb{F}_1\{\mathbb{F}'\} \mid Q_1$, hence the result holds.
- Restriction, locality: similar to the parallel case.

□

We define $\text{fn}(\mathbb{E}) = \text{fn}(\mathbb{E}\{\mathbf{0}\})$.

Lemma 32. *If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ then $fn(\mathbb{E}) = fn(\mathbb{F})$.*

Proof. By induction on the derivation of $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$. □

Lemma 33. *If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ then $nbh(\mathbb{E}) = nbh(\mathbb{F})$.*

Proof. By induction on the derivation of $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$. □

Corollary 3. *Let $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ and $P \approx^{\bullet}_m Q$. We have $\mathbb{E}\{\Box \mid P\} \approx^{\bullet}_m \mathbb{F}\{\Box \mid Q\}$, $\mathbb{E}\{\nu a.\Box\} \approx^{\bullet}_m \mathbb{F}\{\nu a.\Box\}$, and $\mathbb{E}\{a[\Box]\} \approx^{\bullet}_m \mathbb{F}\{a[\Box]\}$.*

Lemma 34. *If $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$ and $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, then there exists $\mathbb{F}_1, \mathbb{F}_2$ such that $\mathbb{E}_1 \approx^{\bullet}_m \mathbb{F}_1$, $\mathbb{E}_2 \approx^{\bullet}_m \mathbb{F}_2$, and $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$.*

Proof. By induction on $\mathbb{E} \approx^{\bullet}_m \mathbb{F}$

- $\mathbb{E} = \mathbb{E}' \mid P$, $\mathbb{F} = \mathbb{F}' \mid Q$ with $\mathbb{E}' \approx^{\bullet}_{m} \mathbb{F}'$ and $P \approx^{\bullet}_{m} Q$. There exists $\mathbb{E}'_1$ such that $\mathbb{E}' = \mathbb{E}'_1\{\nu c.\mathbb{E}_2\}$ and $\mathbb{E}_1 = \mathbb{E}'_1 \mid P$. By induction there exists $\mathbb{F}'_1$, $\mathbb{F}'_2$ such that $\mathbb{F}' = \mathbb{F}'_1\{\nu c.\mathbb{F}'_2\}$, $\mathbb{F}'_1 \approx^{\bullet}_{m} \mathbb{E}'_1$, and $\mathbb{F}'_2 \approx^{\bullet}_{m} \mathbb{E}_2$. We have $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}'_2\} \mid Q$ with $\mathbb{F}'_1 \mid Q \approx^{\bullet}_{m} \mathbb{E}'_1 \mid P$ by congruence, hence the result holds.
- $\mathbb{E} = \nu a.\mathbb{E}'$, $\mathbb{F} = \nu a.\mathbb{F}'$ with $\mathbb{E}' \approx^{\bullet}_{m} \mathbb{F}'$. If $c = a$, then we have $\mathbb{E}_1 = \Box$ and $\mathbb{E}_2 = \mathbb{E}'$. We define $\mathbb{F}_1 = \Box$ and $\mathbb{F}_2 = \mathbb{F}'$. We have the required result. If $c \neq a$, we use the same scheme as in the parallel case.
- Locality: similar to the parallel case.

□

Lemma 35. *Let $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T \approx^{\bullet}_{m} T'$, and $\mathbb{E} \approx^{\bullet}_{m} \mathbb{F}$, then there exists T'', P'' such that $T' \overset{\tau}{\Rightarrow} T''$, $P \overset{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \overset{\tau}{\Rightarrow} P''$ and $P' \approx^{\bullet}_{m} P''$.*

Proof. By induction on the derivation of $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$.

- $P = \overline{a}\langle R\rangle S$ with $\mathrm{fn}(R) = \widetilde{b}$, $T \xrightarrow{a,R} T_0$, $\mathrm{nbh}(\mathbb{E}) \cap \widetilde{b} = \emptyset$, and $P' = T_0 \mid \mathbb{E}\{S\}$. By Lemma 30 there exists T'' such that $T' \overset{a,R}{\Longrightarrow} T''$ and $T_0 \approx^{\bullet}_{m} T''$. There exists T_1, T_2 such that $T' \overset{\tau}{\Rightarrow} T_1 \xrightarrow{a,R} T_2 \overset{\tau}{\Rightarrow} T''$. Because $\mathbb{E} \approx^{\bullet}_{m} \mathbb{F}$, we have $\mathrm{nbh}(\mathbb{E}) = \mathrm{nbh}(\mathbb{F})$ by Lemma 33, therefore we have $\mathrm{nbh}(\mathbb{F}) \cap \widetilde{b} = \emptyset$. By rule $\textsc{Out}^{p}_{o}$, we have $P \xrightarrow{\overline{a},T_1,\mathbb{F}}_{\widetilde{b}} T_2 \mid \mathbb{F}\{S\}$. With $T_2 \overset{\tau}{\Rightarrow} T''$, we have $T_2 \mid \mathbb{F}\{S\} \overset{\tau}{\Rightarrow} T'' \mid \mathbb{F}\{S\}$ by rule $\textsc{Par}^{p}_{i\tau}$, so finally we have $P \xrightarrow{\overline{a},T_1,\mathbb{F}}_{\widetilde{b}} T'' \mid \mathbb{F}\{S\} = P''$ with $T' \overset{\tau}{\Rightarrow} T_1$. Since $\approx^{\bullet}_{m}$ is a congruence, we have $P' \approx^{\bullet}_{m} P''$, as required.
- $P = b[P_1]$ and passivation occurs: similar to the case above.
- $P = b[P_1]$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}\{b[\Box]\}}_{\widetilde{b}} P'_1$. By induction there exists T'', P''_1 such that $P_1 \overset{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}\{b[\Box]\}}_{\widetilde{b}} \overset{\tau}{\Rightarrow} P''_1$ with $T' \overset{\tau}{\Rightarrow} T''$, and $P'_1 \approx^{\bullet}_{m} P''_1$. By rules $\textsc{Loc}^{p}_{i\tau}$ and $\textsc{Loc}^{p}_{o}$, we have $P \overset{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \overset{\tau}{\Rightarrow} P''_1$ with $P'_1 \approx^{\bullet}_{m} P''_1$ as wished.
- Parallel, replication: similar to the case above.
- $P = \nu c.P_1$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}\{\nu y.\Box\}}_{\widetilde{b}} P'_1$, $y \notin \widetilde{b}$. Similar to the case above.
- $P = \nu c.P_1$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}}_{c\cup\widetilde{b}} P'_1$. By induction there exists T'', P''_1 such that $P_1 \overset{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{c\cup\widetilde{b}} \overset{\tau}{\Rightarrow} P''_1$, $T' \overset{\tau}{\Rightarrow} T''$, and $P'_1 \approx^{\bullet}_{m} P''_1$. Using $\textsc{Restr}^{p}_{i\tau}$ for silent actions and $\textsc{Extr}^{p}_{o}$, we have $P \overset{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \overset{\tau}{\Rightarrow} \nu c.P''_1$. Since $\approx^{\bullet}_{m}$ is a congruence, we have $\nu c.P'_1 \approx^{\bullet}_{m} \nu c.P''_1$, as required.

□

Lemma 36. *Let $P\ (\approx_m)_c^\bullet\ Q$. If $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T\ (\approx_m)_c^\bullet\ T'$, and $\mathbb{E}\ (\approx_m)_c^\bullet\ \mathbb{F}$, then there exists T'', Q' such that $T' \stackrel{\tau}{\Rightarrow} T$", $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$.*

Proof. We proceed by induction on the size of the derivation of $P\ (\approx_m)_c^\bullet\ Q$.

- Suppose $P \approx_m^\circ Q$. Since P, Q are closed, we have $P \approx_m Q$. By Lemma 35, there exists T'', P'' such that $T' \stackrel{\tau}{\Rightarrow} T''$, $P \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''$ and $P' \approx_m^\bullet P''$. By Lemma 24, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} \stackrel{\overline{a},T'',\mathbb{F}}{\longmapsto}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$ and $P'' \approx_m Q'$. Since the involved processes are closed, P" is closed, so we have $P' \approx_m^\bullet \approx_m^\circ Q'$, and since the involved processes are closed, we have $P'\ (\approx_m)_c^\bullet\ Q'$ as required.
- Suppose $P \approx_m^\bullet R \approx_m^\circ Q$. Let σ be a substitution that closes R. Since P is closed, we have $P \approx_m^\bullet R\sigma$ by Lemma 29. Since Q is closed, we have $R\sigma \approx_m Q$ by open extension definition. By induction, there exists $T", R'$ such that $T' \stackrel{\tau}{\Rightarrow} T"$, $R\sigma \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} R'$ and $P'\ (\approx_m)_c^\bullet\ R'$. By Lemma 24, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$ and $R' \approx_m Q'$. Since R', Q' are closed, we have $R' \approx_m^\circ Q'$, consequently we have $P' \approx_m^\bullet \approx_m^\circ Q'$. The involved processes are closed, hence we have $P'\ (\approx_m)_c^\bullet\ Q'$ as wished.
- If $P = op(\widetilde{P})$ and $Q = op(\widetilde{Q})$ with $\widetilde{P}\ (\approx_m)_c^\bullet\ \widetilde{Q}$.
  - $P = \overline{a}\langle P_1\rangle P_2$ and $Q = \overline{a}\langle Q_1\rangle Q_2$ with $T \stackrel{a,P_1}{\longmapsto} U$, $\widetilde{b} = \mathrm{fn}(P_1)$, and $P' = U \mid \mathbb{E}\{P_2\}$. Since $P_1\ (\approx_m)_c^\bullet\ Q_1$, we also have $\mathrm{fn}(Q_1) = \widetilde{b}$. By Lemma 30 there exists U' such that $T' \stackrel{a,Q_1}{\Longmapsto} U'$ and $U\ (\approx_m)_c^\bullet\ U'$. There exists U_1, U_2 such that $T' \stackrel{\tau}{\Rightarrow} U_1 \stackrel{a,Q_1}{\longmapsto} U_2 \stackrel{\tau}{\Rightarrow} U'$. Consequently we have $Q \xrightarrow{\overline{a},U_1,\mathbb{F}}_{\widetilde{b}} U_2 \mid \mathbb{F}\{Q_2\}$. We have $T' \stackrel{\tau}{\Rightarrow} U_1$ and $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},U_1,\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} U' \mid \mathbb{F}\{Q_2\} = Q'$. We have $P_2\ (\approx_m)_c^\bullet\ Q_2$ and $\mathbb{E}\ (\approx_m)_c^\bullet\ \mathbb{F}$, so we have $\mathbb{E}\{P_2\}\ (\approx_m)_c^\bullet\ \mathbb{F}\{Q_2\}$ by Lemma 31, hence we have $P'\ (\approx_m)_c^\bullet\ Q'$, as required.
  - $P = b[P_1]$ with passivation: similar to the case above.
  - $P = P_1 \mid P_2$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}\{\Box \mid P_2\}}_{\widetilde{b}} P'$. Since $P_2\ (\approx_m)_c^\bullet\ Q_2$ we have $\mathbb{E}\{\Box \mid P_2\}\ (\approx_m)_c^\bullet\ \mathbb{F}\{\Box \mid Q_2\}$. By induction there exists $T", Q'$ such that $T' \stackrel{\tau}{\Rightarrow} T"$, $Q_1 \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T",\mathbb{F}\{\Box \mid Q_2\}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$. By rules $\textsc{Par}_{i\tau}^p$ and $\textsc{Par}_o^p$ we have $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T",\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$, as required.
  - $P = b[P_1]$ without passivation: similar to the case above.
  - $P = !P_1$: similar to the case above.
  - $P = \nu c.P_1$ with $P_1 \xrightarrow{\overline{c},f,a}_T \mathbb{E}\{\nu c.\Box\}\widetilde{b}P_1'$ and $c \notin \widetilde{b}$. Similar to the case above.

– $P = \nu c.P_1$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}}_{c\cup\widetilde{b}} P_1'$. By induction there exists $T", Q_1'$ such that $T' \stackrel{\tau}{\Rightarrow} T"$, $Q_1 \stackrel{\tau}{\Rightarrow}\xrightarrow{\overline{a},T',\mathbb{F}}_{c\cup\widetilde{b}}\stackrel{\tau}{\Rightarrow} Q_1'$ and $P_1' \ (\approx_m)_c^\bullet \ Q_1'$. By rules $\textsc{Par}_{i\tau}^p$ and $\textsc{Extr}_o^p$ we have $Q \stackrel{\tau}{\Rightarrow}\xrightarrow{\overline{a},T",\mathbb{F}}_{\widetilde{b}}\stackrel{\tau}{\Rightarrow} \nu c.Q_1'$. Since $\approx_m^\bullet$ is a congruence and the involved processes are closed, we have $\nu c.P_1' \ (\approx_m)_c^\bullet \ \nu c.Q_1'$, as required.

□

Lemma 37. *Let $P \ (\approx_m)_c^\bullet \ Q$. If $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T \ (\approx_m)_c^\bullet \ T'$, and $\mathbb{E} \ (\approx_m)_c^\bullet \ \mathbb{F}$, then there exists Q' such that $Q \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} Q'$ and $P' \ (\approx_m)_c^\bullet \ Q'$.*

Proof. We proceed by induction on the number of names in $\widetilde{b} \cap \mathrm{nbh}(\mathbb{E})$.

If this number is zero, the transition $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$ comes from rule $\textsc{CFree}_o^p$; we have $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$. By Lemma 36, there exists $T", Q'$ such that $T' \stackrel{\tau}{\Rightarrow} T"$, $Q \stackrel{\tau}{\Rightarrow}\xrightarrow{\overline{a},T",\mathbb{F}}_{\widetilde{b}}\stackrel{\tau}{\Rightarrow} Q'$, and $P' \ (\approx_m)_c^\bullet \ Q'$. Using rule $\textsc{CFree}_o^p$ we have $Q \stackrel{\tau}{\Rightarrow}\xrightarrow{\overline{a},T",\mathbb{F}}_{\widetilde{b}}\stackrel{\tau}{\Rightarrow} Q'$, so we have $Q \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} Q'$, as wished.

Otherwise, the derivation comes from rule $\textsc{Capt}_o^p$: we have $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, $c \in \widetilde{b}$, $P' = \nu c.P_1'$ and $P \xrightarrow{\overline{a},T,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}} P_1'$. By Lemma 34 there exists $\mathbb{F}_1, \mathbb{F}_2$ such that $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$, $\mathbb{F}_1 \approx_m^\bullet \mathbb{E}_1$, and $\mathbb{F}_2 \approx_m^\bullet \mathbb{E}_2$. By induction there exists Q_1' such that $Q \xRightarrow{\overline{a},T',\mathbb{F}_1\{\mathbb{F}_2\}}_{\widetilde{b}} Q_1'$ and $P_1' \approx_m^\bullet Q_1'$. By rule $\textsc{Capt}_o^p$ we have $Q \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} \nu c.Q_1' = Q'$. By congruence, we have $P' \ (\sim_m)_c^\bullet \ Q'$, as wished.

□

Lemma 38. *Let $P \ (\approx_m)_c^\bullet \ Q$. If $P \stackrel{\tau}{\mapsto} P'$ then there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \ (\approx_m)_c^\bullet \ Q'$.*

Proof. We proceed by induction on the size of the derivation of $P \ (\approx_m)_c^\bullet \ Q$.

- Suppose $P \approx_m^\circ Q$. Since P, Q are closed, we have $P \approx_m Q$. The result holds by bisimilarity definition (and since the processes are closed).
- Suppose $P \approx_m^\bullet R \approx_m^\circ Q$. Let σ be a substitution that closes R. Since P is closed, we have $P \approx_m^\bullet R\sigma$ by Lemma 29. Since Q is closed, we have $R\sigma \approx_m Q$ by open extension definition. By induction, there exists R' such that $R\sigma \stackrel{\tau}{\Rightarrow} R'$ and $P' \ (\approx_m)_c^\bullet \ R'$. By Lemma 24, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $R' \approx_m Q'$. Since R', Q' are closed, we have $R' \approx_m^\circ Q'$, consequently we have $P' \approx_m^\bullet \approx_m^\circ Q'$. The involved processes are closed, hence we have $P' \ (\approx_m)_c^\bullet \ Q'$ as wished.
- If $P = op(\widetilde{P})$ and $Q = op(\widetilde{Q})$ with $\widetilde{P} \ (\approx_m)_c^\bullet \ \widetilde{Q}$.
  - $P = P_1 \mid P_2$ with $P_1 \stackrel{\tau}{\mapsto} P_1'$. By induction there exists Q_1' such that $Q_1 \stackrel{\tau}{\Rightarrow} Q_1'$ and $P_1' \ (\approx_m)_c^\bullet \ Q_1'$. Using rule $\textsc{Par}_{i\tau}^p$, we have $Q \stackrel{\tau}{\Rightarrow} Q_1' \mid Q_2$ and since $\approx_m^\bullet$ is a congruence and the involved processes are closed, we have $P_1' \mid P_2 \ (\approx_m)_c^\bullet \ Q_1' \mid Q_2$ as required.

– Locality, restriction, replication without communication: similar to the case above.
– Communication: $P = P_1 \mid P_2$ with $P_1 \overset{\overline{a},P_2,\Box}{\longmapsto}_{\widetilde{b}} P'$. Since $P_1\ (\approx_m)_c^\bullet\ Q_1$ and $P_2\ (\approx_m)_c^\bullet\ Q_2$, there exists Q' such that $Q_1 \overset{\overline{a},Q_2,\Box}{\Longmapsto}_{\widetilde{b}} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$ by Lemma 37. We have $Q_1 \overset{\tau}{\Rightarrow} Q_1' \overset{\overline{a},Q_2',\Box}{\longmapsto}_{\widetilde{b}} \overset{\tau}{\Rightarrow} Q'$ and $Q_2 \overset{\tau}{\Rightarrow} Q_2'$. By $\text{PAR}_{i\tau}^p$, we have $Q \overset{\tau}{\Rightarrow} Q_1' \mid Q_2'$; by HO_τ^p and $\text{PAR}_{i\tau}^p$, we have $Q_1' \mid Q_2' \overset{\tau}{\Rightarrow} Q'$. Hence we have $Q \overset{\tau}{\Rightarrow} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$, as required.
– Replication with communication: similar to the case above.

□

Notice that Lemmas 38, 37, and 30 show that $(\approx_m)_c^\bullet$ is a weak complementary simulation.

Lemma 39. *If $P\ (\approx_m)_c^\bullet\ Q$ and $P \overset{\lambda}{\Rightarrow} P'$, there exists Q' such that $Q \overset{\lambda}{\Rightarrow} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$.*

Proof. Similar to the one of Lemma 24, using Lemmas 38, 37, and 30. □

Lemma 40. *Let $(\approx_m^\bullet)^*$ be the reflexive and transitive closure of $\approx_m^\bullet$.*

- *$(\approx_m^\bullet)^*$ is symmetric.*
- *$((\approx_m)_c^\bullet)^*$ is a weak complementary bisimulation.*

Proof. We prove that $(\approx_m^\bullet)^{-1} \subseteq (\approx_m^\bullet)^*$ by induction on the derivation of $P(\approx_m^\bullet)^{-1}Q$.

- If we have $Q \approx_m^\circ P$, then we have $P \approx_m^\circ Q$, i.e. we have $P(\approx_m^\bullet)^*Q$, as required.
- If we have $Q \approx_m^\bullet T \approx_m^\circ P$, by induction we have $T(\approx_m^\bullet)^*Q$. We have $P \approx_m^\circ T$, i.e. we have $P \approx_m^\bullet T$, so by transitivity we have $P(\approx_m^\bullet)^*Q$, as required.
- If we have $Q = Q_1 \mid Q_2$, $P = P_1 \mid P_2$ with $Q_1 \approx_m^\bullet P_1$ and $Q_2 \approx_m^\bullet P_2$. By induction we have $P_1(\approx_m^\bullet)^*Q_1$ and $P_2(\approx_m^\bullet)^*Q_2$. Since $\approx_m^\bullet$ is a congruence, we have $P_1 \mid P_2(\approx_m^\bullet)^*Q_1 \mid P_2$ and $Q_1 \mid P_2(\approx_m^\bullet)^*Q_1 \mid Q_2$, consequently we have $P(\approx_m^\bullet)^*Q$ by transitivity. The cases for other operators are similar.

We now prove that $((\approx_m)_c^\bullet)^*$ is a weak complementary bisimulation. Since $(\approx_m^\bullet)^*$ is symmetric, it is enough to prove that $((\approx_m)_c^\bullet)^*$ is a weak complementary simulation. Let $P((\approx_m)_c^\bullet)^*Q$; there exists k such that $P((\approx_m)_c^\bullet)^kQ$. We proceed by induction on k. The result holds for $k = 0$, suppose it holds for $l \leq k$, we prove for $k+1$. Let $P((\approx_m)_c^\bullet)^kP_k\ (\approx_m)_c^\bullet\ Q$.

- $\text{fn}(P) = \text{fn}(P_k) = \text{fn}(Q)$

- If $P \stackrel{\lambda}{\mapsto} P'$, then by induction there exists a process P'_k such that $P_k \stackrel{\lambda}{\Mapsto} P'_k$ and $P'((\approx_m)^\bullet_c)^* P'_k$. By Lemma 39, there exists Q' such that $Q \stackrel{\lambda}{\Mapsto} Q'$ and $P'_k \ (\approx_m)^\bullet_c \ Q'$. The result then holds by transitivity.

□

Theorem 17 (**Theorem 8**). *$\approx_m$ is a congruence.*

Proof. We have $\approx_m \subseteq ((\approx_m)^\bullet_c)^* \subseteq \approx_m$, hence $((\approx_m)^\bullet_c)^* = \approx_m$, and $((\approx_m)^\bullet_c)^*$ is a congruence. □

Appendix A.3. Completeness

We now prove the completeness of $\approx_m$ on image-finite processes. The method is standard [39] and relies on a decomposition of $\approx_m$ into a family of relations $(\approx^k_m)_{k\geq 0}$.

Definition 23. *We define $(\approx^k_m)_{k\geq 0}$ as:*

- *we have $P \approx^0_m Q$ iff $fn(P) = fn(Q)$;*
- *we have $P \approx^{k+1}_m Q$ iff $fn(P) = fn(Q)$ and for all $P \stackrel{\lambda}{\mapsto} P'$, there exists Q' such that $Q \stackrel{\lambda}{\Mapsto} Q'$ and $P' \approx^k_m Q'$, and conversely for $Q \stackrel{\lambda}{\mapsto} Q'$.*

The relation $\approx^\omega_m$ is defined as $\approx^\omega_m \stackrel{\Delta}{=} \bigcap_{k\in\mathcal{N}} \approx^k_m$.

Roughly, we have $P \approx^k_m Q$ iff P and Q can mimic each others on k transition steps. Note that for all k, we have $\approx_{k+1} \subseteq \approx_k$ by definition.

Lemma 41. *We have $\approx_m = \approx^\omega_m$ on image-finite processes.*

Proof. By definition of $\approx^\omega_m$, we have $\approx_m \subseteq \approx^\omega_m$. We prove the reverse inclusion on image-finite processes by showing that $\approx^\omega_m$ is an early weak complementary bisimulation.

Suppose $P \stackrel{\lambda}{\mapsto} P'$. For all k, there exists Q'_k such that $Q \stackrel{\lambda}{\Mapsto} Q'_k$ and $P' \approx^k_m Q'_k$. Because Q is image-finite, there exists Q' such that $Q \stackrel{\lambda}{\Mapsto} Q'$ and $Q' = Q_k$ for an infinite set of k. We have then $P' \approx^k_m Q'$ for an infinite set of k, therefore we have $P' \approx^\omega_m Q'$.

□

Lemma 42. *If $R \stackrel{a,P}{\longmapsto} R''$, then there exists $\mathbb{E}$ and $a(X)R'$ such that $R \equiv \mathbb{E}\{a(X)R'\}$ and $R'' = \mathbb{E}\{R'\{P/X\}\}$.*

Proof. Easy by induction on R.

□

The following result adds observable actions to a transition $P \stackrel{\overline{a},R,\mathbb{E}}{\longmapsto\!\!\!\!\!\!\sim_{\widetilde{b}}} P'$.

Lemma 43. *For all $P \stackrel{\overline{a},R,\mathbb{E}}{\longmapsto\!\!\!\!\!\!\sim_{\widetilde{b}}} P'$, there exists $R_c = \mathbb{F}\{R'\} \mid \overline{c}.\mathbf{0}$ such that $R \equiv \mathbb{F}\{a(X)R'\}$ and*

- $P \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} \equiv P' \mid \overline{c}.\mathbf{0}$;
- *for all* Q *such that* $Q \overset{\overline{a},R,\mathbb{E}}{\Longmapsto}_{\widetilde{b}}$, *there exist* Q', Q_c *such that* $Q \overset{\overline{a},a(X)R_c,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q_c$, $Q \overset{\overline{a},R,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'$ *and* $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$.

Proof. We prove that R' exists and the first item by induction on $P \overset{\overline{a},R,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$. For rule $\textsc{CFree}^p_o$, we have $P \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'$; we prove by induction on $P \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'$ that there exists R_c such that $P \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \equiv P' \mid \overline{c}.\mathbf{0}$.

For rule $\textsc{Out}^p_o$, we have $P = \overline{a}\langle P_1\rangle P_2 \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} R_1 \mid \mathbb{E}\{P_2\} = P'$ with $R \overset{a,P_1}{\longmapsto} R_1$. There exists $\mathbb{F}$, $a(X)R'$ such that $R \equiv \mathbb{F}\{a(X)R'\}$ and $R_1 = \mathbb{F}\{R'\{P_1/X\}\}$. Let $R_c = \mathbb{F}\{R'\} \mid \overline{c}.\mathbf{0}$. We have $a(X)R_c \overset{a,P_1}{\longmapsto} R_1 \mid \overline{c}.\mathbf{0}$, hence we have $P \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} R_1 \mid \overline{c}.\mathbf{0} \mid \mathbb{E}\{P_2\} \equiv P' \mid \overline{c}.\mathbf{0}$, as required. The case $\textsc{Passiv}^p_o$ is treated similarly.

For rule $\textsc{Par}^p_o$, we have $P = P_1 \mid P_2 \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'$ with $P_1 \overset{\overline{a},R,\mathbb{E}\{\Box\mid P_2\}}{\longrightarrow}_{\widetilde{b}} P'$. By induction, there exists R_c such that $P_1 \overset{\overline{a},a(X)R_c,\mathbb{E}\{\Box\mid P_2\}}{\longrightarrow}_{\widetilde{b}} \equiv P' \mid c.\mathbf{0}$. We have then $P \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \equiv P' \mid \overline{c}.\mathbf{0}$, as wished. The cases $\textsc{Restr}^p_o$, $\textsc{Replic}^p_o$, and $\textsc{Loc}^p_o$ are treated similarly.

For rule $\textsc{Extr}^p_o$, we have $P = \nu d.P_1 \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \nu d.P_1' = P'$ with $P_1 \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P_1'$. By induction, there exists R_c such that $P_1 \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \equiv P_1' \mid \overline{c}.\mathbf{0}$. We have $P \overset{\overline{a},R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \equiv \nu d.(P_1' \mid \overline{c}.\mathbf{0}) \equiv (\nu d.P_1') \mid \overline{c}.\mathbf{0} = P' \mid \overline{c}.\mathbf{0}$, hence the result holds.

We now go back to the case $\textsc{CFree}^p_o$ of the induction on $P \overset{\overline{a},R,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$. By the intermediary result on $P \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'$, there exists R_c such that $P \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \equiv P' \mid \overline{c}.\mathbf{0}$. Therefore, we have $P \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} \equiv P' \mid c.\mathbf{0}$ by rule $\textsc{CFree}^p_o$.

For rule $\textsc{Capt}^p_o$, we have $P \overset{\overline{a},R,\mathbb{E}_1\{\nu d.\mathbb{E}_2\}}{\longmapsto}_{\widetilde{b}} \nu d.P_1' = P'$ with $P \overset{\overline{a},R,\mathbb{E}_1\{\mathbb{E}_2\}}{\longmapsto}_{\widetilde{b}} P_1'$. By induction, there exists R_c such that $P \overset{\overline{a},a(X)R_c,\mathbb{E}_1\{\mathbb{E}_2\}}{\longmapsto}_{\widetilde{b}} \equiv P_1' \mid \overline{c}.\mathbf{0}$. For rule $\textsc{Capt}^p_o$, we have $P \overset{\overline{a},a(X)R_c,\mathbb{E}_1\{\nu d.\mathbb{E}_2\}}{\longmapsto}_{\widetilde{b}} \equiv \nu d.(P_1' \mid \overline{c}.\mathbf{0}) \equiv (\nu d.P_1) \mid \overline{c}.\mathbf{0} = P' \mid \overline{c}.\mathbf{0}$, as required.

Let Q such that $Q \overset{\overline{a},R,\mathbb{E}}{\Longmapsto}_{\widetilde{b}}$; by definition there exist R_1, Q_1 such that $R \overset{\tau}{\Longmapsto} R_1$ and $Q \overset{\tau}{\Longmapsto} Q_1 \overset{\overline{a},R_1,\mathbb{E}}{\longmapsto}_{\widetilde{b}} \overset{\tau}{\Longmapsto}$. We prove by induction on $Q_1 \overset{\overline{a},R_1,\mathbb{E}}{\longmapsto}_{\widetilde{b}}$ that there exist Q', Q_c' such that $Q_1 \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} Q_c'$, $Q_1 \overset{\overline{a},R,\mathbb{E}}{\longmapsto}_{\widetilde{b}} Q'$, and $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$.

If the transition comes from $\textsc{CFree}^p_o$, we have $Q \overset{\overline{a},R_1,\mathbb{E}}{\longrightarrow}_{\widetilde{b}}$. We prove by induction on $Q_1 \overset{\overline{a},R_1,\mathbb{E}}{\longrightarrow}_{\widetilde{b}}$ that there exists Q', Q_c' such that $Q_1 \overset{\overline{a},a(X)R_c,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} Q_c'$, $Q_1 \overset{\overline{a},R,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} Q'$ and $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$.

For rule $\textsc{Out}_o^p$, we have $Q_1 = \overline{a}\langle Q^1\rangle Q^2 \xrightarrow{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}} R_1' \mid \mathbb{E}\{Q^2\}$ with $R_1 \xmapsto{a,Q^1} R_1'$. We have $R_c = \mathbb{F}\{R'\} \mid \overline{c}.\mathbf{0}$ and $R \equiv \mathbb{F}\{a(X)R'\}$, hence we have $a(X)R_c \xmapsto{a,Q^1} R_c'$ and $R \xmapsto{a,Q^1} R''$ with $R_c' = R'' \mid \overline{c}.\mathbf{0}$. Therefore we have $Q_1 \xrightarrow{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} R_c' \mid \mathbb{E}\{Q^2\} \triangleq Q_c$ and $Q_1 \xrightarrow{\overline{a},R,\mathbb{E}}_{\widetilde{b}} R'' \mid \mathbb{E}\{Q^2\} \triangleq Q'$. Hence we have $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$, as required. The case $\textsc{Passiv}_o^p$ is treated similarly.

For rule $\textsc{Par}_o^p$, we have $Q_1 = Q^1 \mid Q^2 \xrightarrow{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}}$ with $Q^1 \xrightarrow{\overline{a},R_1,\mathbb{E}\{\Box\mid P_2\}}_{\widetilde{b}}$. By induction, there exist Q', Q_c such that $Q_1 \xmapsto{\overline{a},a(X)R_c,\mathbb{E}\{\Box\mid Q^2\}}_{\widetilde{b}} Q_c$, $Q_1 \xmapsto{\overline{a},R,\mathbb{E}\{\Box\mid Q^2\}}_{\widetilde{b}} Q'$, and $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$. We have $Q \xrightarrow{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} Q_c$ and $Q \xrightarrow{\overline{a},R,\mathbb{E}}_{\widetilde{b}} Q'$, as wished. The cases $\textsc{Restr}_o^p$, $\textsc{Loc}_o^p$, and $\textsc{Replic}_o^p$ are treated similarly.

For rule $\textsc{Extr}_o^p$, we have $Q_1 = \nu d.Q^1 \xrightarrow{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}\setminus d}$ avec $Q^1 \xrightarrow{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}}$. By induction, there exist Q_c^1, Q'^1 such that $Q_1 \xmapsto{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} Q_c^1$, $Q_1 \xmapsto{\overline{a},R,\mathbb{E}}_{\widetilde{b}} Q'^1$, and $Q_c^1 \equiv Q'^1 \mid \overline{c}.\mathbf{0}$. Therefore we have $Q \xmapsto{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}\setminus d} \nu d.Q_c^1 \triangleq Q_c$ and $Q \xrightarrow{\overline{a},R,\mathbb{E}}_{\widetilde{b}} \nu d.Q'^1 \triangleq Q'$. We have $Q_c = \nu d.Q_c^1 \equiv \nu d.(Q'^1 \mid \overline{c}.\mathbf{0}) \equiv (\nu d.Q'^1) \mid \overline{c}.\mathbf{0} = Q' \mid \overline{c}.\mathbf{0}$, hence the result holds.

We now go back to the case $\textsc{CFree}_o^p$ of the induction on $Q_1 \xmapsto{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}}$. By the intermediary result on $Q \xrightarrow{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}}$, there exist Q', Q_c' such that $Q_1 \xrightarrow{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} Q_c'$, $Q_1 \xrightarrow{\overline{a},R,\mathbb{E}}_{\widetilde{b}} Q'$ et $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$. By rule $\textsc{CFree}_o^p$, we have $Q_1 \xmapsto{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} Q_c'$ and $Q_1 \xmapsto{\overline{a},R,\mathbb{E}}_{\widetilde{b}} Q'$, hence the result holds.

In the case of rule $\textsc{Capt}_o^p$, we have $Q \xmapsto{\overline{a},R_1,\mathbb{E}}_{\widetilde{b}}$ with $Q \xmapsto{\overline{a},R_1,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}}$ and $\mathbb{E} = \mathbb{E}_1\{\nu d.\mathbb{E}_2\}$. By induction, there exist Q'', Q_c'' such that $Q_1 \xmapsto{\overline{a},a(X)R_c,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}} Q_c''$, $Q_1 \xrightarrow{\overline{a},R,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}} Q''$ and $Q_c' \equiv Q'' \mid \overline{c}.\mathbf{0}$. By rule $\textsc{Capt}_o^p$, we have $Q_1 \xmapsto{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} \nu d.Q_c'' \triangleq Q_c'$ and $Q_1 \xrightarrow{\overline{a},R,\mathbb{E}}_{\widetilde{b}} \nu d.Q'' \triangleq Q'$. We have $Q_c' \equiv \nu d.(Q'' \mid \overline{c}.\mathbf{0}) \equiv (\nu d.Q'') \mid \overline{c}.\mathbf{0} = Q' \mid \overline{c}.\mathbf{0}$, as wished.

We are now done with the induction; there exist Q' and Q_c' such that $Q_1 \xmapsto{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} Q_c'$, $Q_1 \xmapsto{\overline{a},R,\mathbb{E}}_{\widetilde{b}} Q'$, and $Q_c \equiv Q' \mid \overline{c}.\mathbf{0}$. We have $Q \overset{\tau}{\Longmapsto} \xmapsto{\overline{a},a(X)R_c,\mathbb{E}}_{\widetilde{b}} Q_c'$ and $Q \overset{\tau}{\Longmapsto} \xmapsto{\overline{a},R,\mathbb{E}}_{\widetilde{b}} Q'$, i.e., $Q \overset{\overline{a},a(X)R_c,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q_c'$ and $Q \overset{\overline{a},R,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'$, as wished.

□

In the following, we omit the trailing $\mathbf{0}$; in particular, we write a for $a.\mathbf{0}$. We define an operator $\oplus$ as:

$$\bigoplus_{j=1}^{n} P_j \quad \triangleq \quad \nu a.(\overline{a}\langle P_1\rangle\mathbf{0} \mid \ldots \mid \overline{a}\langle P_n\rangle\mathbf{0} \mid a(X)X \mid \prod_{j=2}^{n} a(X_j)\mathbf{0})$$

The operator $\oplus$ is a choice operator; once a process P_i is chosen (i.e., received by $a(X)X$), the process $\prod_{j=2}^{n} a(X_j)\mathbf{0}$ destroys the remaining processes P_j for

$j \neq i$. It is necessary to remove the free names of the processes $(P_j)_{j\neq i}$, in order to obtain P' such that $P' \approx_m P_i$.

The operator $\oplus$ has the following property:

- $P \oplus a \downarrow_a$;
- for all $i \in \{1 \dots n\}$, we have $\bigoplus_{j=1}^{n} P_j \stackrel{\tau}{\Rightarrow} \approx_m P_i$.

Lemma 44. *Let P, Q be image-finite processes. For all k, if $P \not\approx_m^k Q$, then there exist $\mathbb{C}, e$ such that $\mathbb{C}\{P\} \oplus e \not\approx_b \mathbb{C}\{Q\} \oplus e$.*

Proof. We proceed by induction on k. For $k = 0$, we have $\mathrm{fn}(P) \neq \mathrm{fn}(Q)$; suppose we have $a \in \mathrm{fn}(P) \setminus \mathrm{fn}(Q)$. We define

$$\mathbb{C} \stackrel{\Delta}{=} b[\nu a.(\overline{c}\langle\Box\rangle\mathbf{0} \mid a \mid \overline{a}.\overline{a}.d)] \mid c(X)b(Y)(Y \mid Y)$$

with b, c, d not free in P and Q. Let e be a fresh name; assume $\mathbb{C}\{P\} \oplus e \approx_b \mathbb{C}\{Q\} \oplus e$ holds. By communication on c, we have

$$\mathbb{C}\{P\} \oplus e \stackrel{\tau}{\Rightarrow} \nu a.(b[a \mid \overline{a}.\overline{a}.d] \mid b(Y)(Y \mid Y)) \stackrel{\Delta}{=} P_1$$

Because a is free in P, the scope of νa is extended outside b. The name b is observable in P_1 but c is not, therefore this transition can only be matched by

$$\mathbb{C}\{Q\} \oplus e \stackrel{\tau}{\Rightarrow} b[\nu a.R_a] \mid b(Y)(Y \mid Y) \stackrel{\Delta}{=} Q_1$$

with $R_a = a \mid \overline{a}.\overline{a}.d$ ou $R_a = \overline{a}.d$. We have

$$P_1 \stackrel{\tau}{\mapsto} \nu a.(a \mid \overline{a}.\overline{a}.d \mid a \mid \overline{a}.\overline{a}.d) \stackrel{\Delta}{=} P_2$$

by passivation of b. Because b is no longer observable in P_2, this can only be matched by

$$Q_1 \stackrel{\tau}{\Rightarrow} (\nu a.R'_a) \mid (\nu a.R''_a) \stackrel{\Delta}{=} Q_2$$

with $R_a \stackrel{\tau}{\Rightarrow} R'_a$ et $R_a \stackrel{\tau}{\Rightarrow} R''_a$. The transition $P_2 \stackrel{\tau}{\Rightarrow} \nu a.(d \mid \overline{a}.\overline{a}.d)$ cannot be matched by Q_2, because processes R'_a and R''_a have their own copy of a and cannot synchronize themselves to make d observable. Hence we have a contradiction, and $\mathbb{C} \oplus e$ distinguishes P and Q.

Assume that the result holds for $l \leq k$. Let $P \not\approx_{k+1} Q$; we distinguish three cases.

If $P \stackrel{\tau}{\mapsto} P'$, then for all Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$, we have $P' \not\approx_m^k Q'$. Because Q is image-finite, the set $\{Q_i, Q \stackrel{\tau}{\Rightarrow} Q_i\}$ is finite. By induction, there exist $\mathbb{C}_i, e_i$ such that $\mathbb{C}_i\{P'\} \oplus e_i \not\approx_b \mathbb{C}_i\{Q_i\} \oplus e_i$ for all i. Let

$$\mathbb{C} \stackrel{\Delta}{=} a[\Box] \mid a(X)(b \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j)$$

with a, b fresh for P, Q. Let e be a fresh name. Suppose $\mathbb{C}\{P\} \oplus e \approx_b \mathbb{C}\{Q\} \oplus e$. We have

$$\mathbb{C}\{P\} \oplus e \stackrel{\tau}{\Mapsto}\approx_m a[P'] \mid a(X)(b \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} P_1$$

The name a is observable in P_1, but t is not, therefore this can only be matched by

$$\mathbb{C}\{Q\} \oplus e \stackrel{\tau}{\Mapsto}\approx_m a[Q'_l] \mid a(X)(b \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} Q_1$$

for some l. We have

$$P_1 \stackrel{\tau}{\mapsto} b \oplus \bigoplus_j \mathbb{C}_j\{P'\} \oplus e_j \stackrel{\Delta}{=} P_2$$

Because b is observable in P_2, this can only be matched by

$$Q_1 \stackrel{\tau}{\Mapsto} b \oplus \bigoplus_j \mathbb{C}_j\{Q'_j\} \oplus e_j \stackrel{\Delta}{=} P_2$$

with $Q'_l \stackrel{\tau}{\Mapsto} Q'_i$. We have $P_2 \stackrel{\tau}{\Mapsto}\approx_m \mathbb{C}_i\{P'\} \oplus e_i \stackrel{\Delta}{=} P_3$; because $P_3 \downarrow_{e_i}$ holds, this can only be matched by $Q_2 \stackrel{\tau}{\Mapsto}\approx_m \mathbb{C}_i\{Q'_i\} \oplus e_i \stackrel{\Delta}{=} Q_3$. We have $\mathbb{C}_i\{P'\} \oplus e_i \not\approx_b \mathbb{C}_i\{Q'_i\} \oplus e_i$, hence a contradiction.

If $P \stackrel{a,R}{\longmapsto} P'$, then for all Q' such that $Q \stackrel{a,R}{\Longmapsto} Q'$, we have $P' \not\approx^k_m Q'$. Because Q is image-finite, the set $\{Q_i, Q \stackrel{a,R}{\Longmapsto} Q_i\}$ is finite. By induction, there exist $\mathbb{C}_i, e_i$ such that $\mathbb{C}_i\{P'\} \oplus e_i \not\approx_b \mathbb{C}_i\{Q_i\} \oplus e_i$ for all i. Let

$$\mathbb{C} \stackrel{\Delta}{=} c[\Box \mid \overline{a}\langle R\rangle\overline{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j)$$

with c, d, f not free in P, Q, R. Let e be a fresh name; we have

$$\mathbb{C}\{P\} \oplus e \stackrel{\tau}{\Mapsto}\approx_m c[P' \mid \overline{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} P_1$$

With observable $\overline{d}$, we are sure that the communication between P and R took place. Because we have $P_1 \downarrow_{\overline{d}}$, this can only be matched with

$$\mathbb{C}\{Q\} \oplus e \stackrel{\tau}{\Mapsto}\approx_m c[Q'_l \mid \overline{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} Q_1$$

for some l. We have

$$P_1 \stackrel{\tau}{\mapsto} c[P'] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} P_2$$

Because $P_2 \downarrow_c$ holds, this can only be matched with

$$Q_1 \stackrel{\tau}{\Mapsto} c[Q_i'] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} Q_2$$

with $Q_l' \stackrel{\tau}{\Mapsto} Q_i'$. From there, the proof is the same as in the previous case.

If $P \stackrel{\overline{a},R,\mathbb{E}}{\longmapsto_{\widetilde{b}}} P'$, then for all Q' such that $Q \stackrel{\overline{a},R,\mathbb{E}}{\Longmapsto_{\widetilde{b}}} Q'$, we have $P' \not\approx_m^k Q'$. Because Q is image-finite, the set $\{Q_i, Q \stackrel{\overline{a},R,\mathbb{E}}{\Longmapsto_{\widetilde{b}}} Q_i\}$ is finite. By induction there exist $\mathbb{C}_i, e_i$ such that $\mathbb{C}_i\{P'\} \oplus e_i \not\approx_b \mathbb{C}_i\{Q_i\} \oplus e_i$ for all i. Let $d \notin \mathrm{fn}(P, Q, R, \mathbb{E})$. By Lemma 43, there exists R_d such that $P \stackrel{\overline{a},a(X)R_d,\mathbb{E}}{\longmapsto_{\widetilde{b}}} \equiv P' \mid \overline{d}.\mathbf{0}$. Let

$$\mathbb{C} \stackrel{\Delta}{=} c[\Box \mid a(X)R_d] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j)$$

with c, f not free in $P, Q, R, \mathbb{E}$. Let e be a fresh name; we have

$$\mathbb{C}\{P\} \oplus e \stackrel{\tau}{\Mapsto} \approx_m c[P' \mid \overline{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} P_1$$

With observable $\overline{d}$, we are sure that the communication between P and R took place. Because we have $P_1 \downarrow_{\overline{d}}$, the process Q communicates with $a(X)R_d$, and the result of this communication is a process Q_l', by Lemma 43. Therefore we have

$$\mathbb{C}\{Q\} \oplus e \stackrel{\tau}{\Mapsto} \approx_m c[Q_l' \mid \overline{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} Q_1.$$

We have

$$P_1 \stackrel{\tau}{\mapsto} c[P'] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} P_2$$

Because $P_2 \downarrow_c$ holds, this can only be matched by

$$Q_1 \stackrel{\tau}{\Mapsto} c[Q_i'] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \stackrel{\Delta}{=} Q_2$$

with $Q_l' \stackrel{\tau}{\Mapsto} Q_i'$. From there, the proof is the same as in the previous cases.

□

Theorem 18 (**Theorem 10**). *Let P, Q be image finite processes. If $P \approx_b Q$, then $P \approx_m Q$.*

Proof. We prove that $P \not\approx_m Q$ implies $P \not\approx_b Q$. Suppose $P \not\approx_m Q$. Because $\approx_m = \approx_\omega$ (Lemma 41), there exists k such that $P \not\approx_m^k Q$. By Lemma 44, there exist $\mathbb{C}, e$ such that $\mathbb{C}\{P\} \oplus e \not\approx_b \mathbb{C}\{Q\} \oplus e$. Therefore, we have $P \not\approx_b Q$.

□

Appendix B. Abstraction Equivalence in HOπP

In this section, we prove that the families of abstractions $(F_n)_{n\geq 0}$, $(G_n)_{n\geq 0}$, defined in Section 6.3, are counter-examples to show that testing using finite processes is not enough to guarantee bisimilarity in HOπP.

Lemma 45. *For all P_F such that $d(P_F) = 0$, we have $F_0 \circ P_F \sim G_0 \circ P_F$.*

Proof. Since $d(P_F) = 0$, P_F and $P_F \mid P_F$ cannot perform any transition. We have $\mathrm{fn}(P_F) = \mathrm{fn}(P_F \mid P_F)$, so we have $F_0 \circ P_F \sim G_0 \circ P_F$.

□

Lemma 46. *Let $n > 0$. For all P_F such that $d(P_F) \leq n$, we have $F_n \circ P_F \sim G_n \circ P_F$.*

Proof. We prove that relation

$$\mathcal{R}_n \stackrel{\Delta}{=} \{(\mathbb{C}\{P\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/\widetilde{X}\}\}, \mathbb{C}\{P\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/\widetilde{X}\}\}), \\ d(P_F^k) \leq k \leq n \wedge d(P_F^l) \leq l - 1 \leq n\}$$

is a strong early context simulation.

Let $P_1 \; \mathcal{R}_n \; P_2$. We proceed by case analysis on the transition initiated by P_1.

If the transition comes from P or $\mathbb{C}$ without any interaction with the processes $F_k \circ P_F^k$, then P_2 matches with the same transition.

The transition comes from a process $F_{k_0} \circ P_F^{k_0}$, in which passivation of locality a_{k_0} has been triggered. We have

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0}.(F_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \stackrel{\Delta}{=} P_1'.$$

We distinguish two cases; suppose first that we have $d(P_F^{k_0}) \leq k_0 - 1$. Process P_2 matches with passivation of a_{k_0} in $G_{k_0} \circ P_F^{k_0}$, i.e.

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0}.(G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \stackrel{\Delta}{=} P_2'.$$

Let $P' \stackrel{\Delta}{=} P\{\nu a_{k_0}.X_{k_0}/X_{k_0}\}$. Processes P_1' and P_2' can be written

$$\begin{aligned} P_1' &= \mathbb{C}\{P'\{\widetilde{F_k \circ P_F^k}, F_{k_0-1} \circ P_F^{k_0}, \widetilde{R_l^1 \circ P_F^l}/\widetilde{X}\}\} \\ P_2' &= \mathbb{C}\{P'\{\widetilde{G_k \circ P_F^k}, G_{k_0-1} \circ P_F^{k_0}, \widetilde{S_l^1 \circ P_F^l}/\widetilde{X}\}\} \end{aligned}$$

and since we have $d(P_F^{k_0}) \leq k_0 - 1 \leq n$, we have $P_1' \; \mathcal{R}_n \; P_2'$, as required.

In the case $d(P_F^{k_0}) = k_0$, process P_2 matches with the τ-action in the subprocess S_{k_0} of $G_{k_0} \circ P_F^{k_0}$. We have then

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0}.(F_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \stackrel{\Delta}{=} P_2'$$

Let $P' \triangleq P\{\nu a_{k_0}.(F_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}$; P'_1 and P'_2 can be written

$$\begin{aligned} P'_1 &= \mathbb{C}\{P'\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \\ P'_2 &= \mathbb{C}\{P'\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \end{aligned}$$

Hence we have $P'_1 \; \mathcal{R}_n \; P'_2$ as required.

The transition from P_1 comes from a process $R_{l_0}^1 \circ P_F^{l_0}$, in which passivation of locality a_{l_0} is triggered. By definition, we have$d(P_F^{l_0}) \leq l_0 - 1$, hence this case is similar to first sub-case of the previous case.

Suppose that the transition from P_1 comes from the τ-action of a process R_{k_0} inside a process $F_{k_0} \circ P_F^{k_0}$. We have then

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0}.(G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq P'_1.$$

Process P_2 matches with passivation of a_{k_0} inside process $G_{k_0} \circ P_F^{k_0}$, i.e.

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0}.(G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq P'_2$$

Let $P' \triangleq P\{\nu a_{k_0}.(G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}$; we rewrite P'_1 and P'_2 in

$$\begin{aligned} P'_1 &= \mathbb{C}\{P'\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \\ P'_2 &= \mathbb{C}\{P'\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \end{aligned}$$

hence we have $P'_1 \; \mathcal{R}_n \; P'_2$.

The transition comes from a process $F_{k_0} \circ P_F^{k_0}$, in which $P_F^{k_0}$ performs an action $P_F^{k_0} \xrightarrow{\tau} P_F'^{k_0}$. We have then

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P\{R_{k_0}^1 \circ P_F'^{k_0}/X_{k_0}\}\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq P'_1.$$

Process P_2 matches with a similar transition

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{S_{k_0}^1 \circ P_F'^{k_0}/X_{k_0}\}\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq P'_2.$$

By the definition of depth, we have $d(P_F'^{k_0}) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$, hence we have $P'_1 \; \mathcal{R}_n \; P'_2$.

The transition from P_1 comes from a process $F_{k_0} \circ P_F^{k_0}$, in which $P_F^{k_0}$ performs an input $P_F^{k_0} \xrightarrow{a} F$. We have then

$$P_1 \xrightarrow{a} \mathbb{C}\{P\{R_{k_0}^1 \circ F/X_{k_0}\}\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq F_1.$$

Let $C = \nu\widetilde{b}.\langle T\rangle U$. Process P_2 matches with a similar transition

$$P_2 \xrightarrow{a} \mathbb{C}\{P\{S^1_{k_0} \circ F/X_{k_0}\}\{\widetilde{G_k \circ P^k_F}, \widetilde{S^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq F_2.$$

We have

$$\begin{aligned} F_1 \bullet C &= \nu\widetilde{b}.(\mathbb{C}\{P\{R^1_{k_0} \circ (F \circ T)/X_{k_0}\}\{\widetilde{F_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \mid U) \\ F_2 \bullet C &= \nu\widetilde{b}.(\mathbb{C}\{P\{S^1_{k_0} \circ (F \circ T)/X_{k_0}\}\{\widetilde{G_k \circ P^k_F}, \widetilde{S^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \mid U) \end{aligned}$$

Let $\mathbb{C}' \triangleq \nu\widetilde{b}.(\mathbb{C} \mid U)$; $F_1 \bullet C$ and $F_2 \bullet C$ can be written

$$\begin{aligned} F_1 \bullet C &= \mathbb{C}'\{P\{R^1_{k_0} \circ (F \circ T)/X_{k_0}\}\{\widetilde{F_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \\ F_2 \bullet C &= \mathbb{C}'\{P\{S^1_{k_0} \circ (F \circ T)/X_{k_0}\}\{\widetilde{G_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \end{aligned}$$

By definition of depth, we have $d(F \circ T) = d(F) \leq d(P^{k_0}_F) - 1 \leq k_0 - 1 \leq n$, hence we have $F_1 \bullet C \; \mathcal{R}_n \; F_2 \bullet C$.

The transition from P_1 comes from a process $F_{k_0} \circ P^{k_0}_F$, in which $P^{k_0}_F$ performs an output $P^{k_0}_F \xrightarrow{\overline{a}} C = \nu\widetilde{b}.\langle T\rangle U$. We have

$$P_1 \xrightarrow{\overline{a}} \nu\widetilde{b}, \widetilde{b'}.\langle T\rangle\mathbb{C}'\{P\{R^1_{k_0} \circ U/X_{k_0}\}\{\widetilde{F_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq C_1$$

where $\widetilde{b'}$ is the set of names captured by $\mathbb{C}$, and $\mathbb{C}'$ is the context resulting from $\mathbb{C}$ after removing the name restrictions on $\widetilde{b'}$. Let F be an abstraction and $\mathbb{E}$ be an evaluation context. Process P_2 matches with the transition

$$P_2 \xrightarrow{\overline{a}} \nu\widetilde{b}, \widetilde{b'}.\langle T\rangle\mathbb{C}'\{P\{S^1_{k_0} \circ U/X_{k_0}\}\{\widetilde{G_k \circ P^k_F}, \widetilde{S^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \triangleq C_2.$$

We have

$$F \bullet \mathbb{E}\{C_1\} =$$
$$\nu\widetilde{b}, \widetilde{b'}, \widetilde{b"}.(F \circ T \mid \mathbb{E}'\{\mathbb{C}'\{P\{R^1_{k_0} \circ U/X_{k_0}\}\{\widetilde{F_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\}\})$$

$$F \bullet \mathbb{E}\{C_2\} =$$
$$\nu\widetilde{b}, \widetilde{b'}, \widetilde{b"}.(F \circ T \mid \mathbb{E}'\{\mathbb{C}'\{P\{S^1_{k_0} \circ U/X_{k_0}\}\{\widetilde{G_k \circ P^k_F}, \widetilde{S^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\}\})$$

where $\widetilde{b"}$ and $\mathbb{E}'$ are defined the ame way as $\widetilde{b'}$ and $\mathbb{C}'$.

Let $\mathbb{C}" \triangleq \nu\widetilde{b}, \widetilde{b'}, \widetilde{b"}.(F \circ T \mid \mathbb{E}'\{\mathbb{C}'\})$; $F \bullet \mathbb{E}\{C_1\}$ and $F \bullet \mathbb{E}\{C_2\}$ can be written

$$\begin{aligned} F \bullet \mathbb{E}\{C_1\} &= \mathbb{C}"\{P\{R^1_{k_0} \circ U/X_{k_0}\}\{\widetilde{F_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \\ F \bullet \mathbb{E}\{C_2\} &= \mathbb{C}"\{P\{S^1_{k_0} \circ U/X_{k_0}\}\{\widetilde{G_k \circ P^k_F}, \widetilde{R^1_l \circ P^l_F}/(\widetilde{X} \setminus X_{k_0})\}\} \end{aligned}$$

By definition of depth we have $d(U) = d(C) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$, hence we have $F \bullet \mathbb{E}\{C_1\} \mathcal{R}_n F \bullet \mathbb{E}\{C_2\}$.

The transition from P_1 comes from the communication between two finite processes, between a finite process and P, or between a finite process and $\mathbb{C}$. We only deal with communication between finite processes, the other cases are similar. Suppose we have $P_F^{k_0} \xrightarrow{a} F$ and $P_F^{k_1} \xrightarrow{\overline{a}} C = \nu \widetilde{b}.\langle T \rangle U$. Then we have

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P'\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}, R_{k_0}^1 \circ (F \circ T), R_{k_1}^1 \circ U/\widetilde{X}, X_{k_0}, X_{k_1}\}\} \triangleq P_1'$$

where P' is obtained from P by scope extrusion of names $\widetilde{b}$. Process P_2 matches with the following transition:

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P'\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}, S_{k_0}^1 \circ (F \circ T), S_{k_1}^1 \circ U/\widetilde{X}, X_{k_0}, X_{k_1}\}\} \triangleq P_2'$$

We have $d(F \circ T) = d(F) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$ and $d(S) = d(C) \leq d(P^{k_1} - 1) - 1 \leq k_1 - 1 \leq n$, hence we have $P_1' \mathcal{R}_n P_2'$, as required.

Similarly, we can prove that $\mathcal{R}_n^1$ is a strong early context bisimilarity.

□

Let (m_k) be a sequence of pairwise distinct fresh names. Let $Q_1 \triangleq m_1.\mathbf{0}$ and $Q_{k+1} \triangleq m_{k+1}.Q_k$ for all $k > 1$.

Lemma 47. *For all n, we have $F_n \circ Q_{n+1} \nsim G_n \circ Q_{n+1}$.*

Proof. We proceed by induction on n. For $n = 0$, we have $F_0 \circ m_1.\mathbf{0} = m_1.\mathbf{0} \nsim m_1.\mathbf{0} \mid m_1.\mathbf{0} = G_0 \circ m_1.\mathbf{0}$, as wished.

Let $n > 0$. We have

$$F_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.F_{n-1}) \triangleq P_1,$$

and $G_n \circ Q_{n+1}$ can match only with transition

$$G_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.G_{n-1}) \triangleq P_2.$$

After passivation of locality a_n, we have

$$P_1 \xrightarrow{\tau} \nu a_n.(F_{n-1} \circ Q_n),$$

and P_2 can match only with

$$P_2 \xrightarrow{\tau} \nu a_n.(G_{n-1} \circ Q_n).$$

Since we have $a_n \notin \mathrm{fn}(F_{n-1} \circ Q_n)$ (respectively $a_n \notin \mathrm{fn}(G_{n-1} \circ Q_n)$), we have $\nu a_n.(F_{n-1} \circ Q_n) \sim F_{n-1} \circ Q_n$ (respectively $\nu a_n.(G_{n-1} \circ Q_n) \sim G_{n-1} \circ Q_n$). By induction, we have $F_{n-1} \circ Q_n \nsim G_{n-1} \circ Q_n$, hence we have $F_n \circ Q_{n+1} \nsim G_n \circ Q_{n+1}$.

□

Appendix C. Normal Bisimilarity in HOP

In this section, we prove the main theorem (Theorem 14) of Section 7.2: testing processes using a trigger is enough to establish bisimilarity in HOP.

Lemma 48. *Let $\mathbb{E}$ be an evaluation context and $P \xrightarrow{\alpha} A$. Then $\mathbb{E}\{P\} \xrightarrow{\alpha} \mathbb{E}'\{A\}$ and the hole in $\mathbb{E}'$ is not under a replication or choice operator.*

Proof. Immediate by induction on $\mathbb{E}$, and considering the rules Par, Loc, Replic, Sum.

□

Lemma 49 (Lemma 14). *Let P, Q such that $fv(P,Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/Y\} = P_n$ matched by $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/Y\} = Q_n$ with $P_n \dot{\sim}_l Q_n$. One of the following holds:*

- *There exists P_1, Q_1 such that $P_n \equiv n.\mathbf{0} \mid P_1$, $Q_n \equiv n.\mathbf{0} \mid Q_1$ with $P_1 \dot{\sim}_l Q_1$.*
- *There exists $a_1, \dots a_k$, $P_1 \dots P_{k+1}$, $Q_1 \dots Q_{k+1}$ such that*

$$P_n \equiv a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$$

and

$$Q_n \equiv a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$$

and for all $1 \leq j \leq k+1$, $P_j \dot{\sim}_l Q_j$.

Proof. Since P_n can only perform one $\xrightarrow{n}$ transition, we can detect if $n.\mathbf{0}$ is in a locality or not: if there exists a transition $P_n \xrightarrow{\overline{a}} \langle R'n\rangle S'_n$ for some a such that R'_n may perform a transition $\xrightarrow{n}$, then the transition is a passivation and the process $n.\mathbf{0}$ is in a locality in P_n. Otherwise, $n.\mathbf{0}$ is not in a locality.

By lemma 48, $n.\mathbf{0}$ is only under localities and parallel compositions in P_n and Q_n.

We show that if $n.\mathbf{0}$ is not under a locality in P_n, it is also not under a locality in Q_n. Suppose $n.\mathbf{0}$ is not in a locality in P_n and is in a locality in Q_n. We have $Q_n \xrightarrow{\overline{a}} \langle \mathbb{E}\{n.\mathbf{0}\}\rangle Q''$ for some $a, \mathbb{E}, Q''$. These transitions can only be matched by a passivation of $n.\mathbf{0}$ in P_n, which is impossible by hypothesis, hence a contradiction. We have the same reasoning if $n.\mathbf{0}$ is in a locality in P_n and not in a locality in Q_n. Therefore if $n.\mathbf{0}$ is not in a locality in P_n, it is not in a locality in Q_n. Consequently in this case, there exists P_1, Q_1 such that $P_n \equiv n.\mathbf{0} \mid P_1$ and $Q_n \equiv n.\mathbf{0} \mid Q_1$. Hence we have $P_n \xrightarrow{n} P_1$, which can only be matched by $Q_n \xrightarrow{n} Q_1$, so we have $P_1 \dot{\sim}_l Q_1$.

We suppose now that $n.\mathbf{0}$ is under a locality in P_n and Q_n. We prove that $n.\mathbf{0}$ is under the same hierarchy of localities in P_n, Q_n, and the existence of the pairwise bisimilar processes defined in the lemma. Suppose $n.\mathbf{0}$ is under k localities $a_1, \dots a_k$ in P_n and under l localities $b_1, \dots b_l$ in Q_n, with $k > l$. We have $P_n \xrightarrow{a_1} \langle P'_1\{n.\mathbf{0}/X_i\}\rangle P_1$, so there exists Q_1, Q'_1 such that $Q_n \xrightarrow{b_i}$

$\langle Q'_1\{n.\mathbf{0}/X_j\}\rangle Q_1$ with $a_1 = b_i$ and $P'_1\{n.\mathbf{0}/X_i\} \dot{\sim}_l Q'_1\{n.\mathbf{0}/X_j\}$. The process is under $k-1$ localities in P'_1 and under $l-i$ localities in Q'_1, with $i \geq 1$. After l passivation, we have P'_l such that the process $n.\mathbf{0}$ is under $k-l$ localities, and a process Q'_l such that the process $n.\mathbf{0}$ is not under a locality and with $P'_l \dot{\sim}_l Q'_l$, which is not possible (same proof as in the first case). If $k < l$, we have a similar contradiction by reasoning on Q, consequently we have $k = l$.

Therefore there exists $a_1 \dots a_k$, $P_1 \dots P_k$, $Q_1 \dots Q_k$, such that $P_n \equiv a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$ and $Q_n \equiv a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$. Let P'_i (resp Q'_i) be the process inside the locality a_i in P_n (resp Q_n). We have $P_n \xrightarrow{\overline{a_1}} \langle P'_1\rangle P_1$, with $P'_1 \xrightarrow{n}$, which is matched by a passivation $Q_n \xrightarrow{\overline{a_i}} \langle Q'_i\rangle Q'$ such that $P_1 \dot{\sim}_l Q'$, $P'_1 \dot{\sim}_l Q'_i$ and $Q'_i \xrightarrow{n}$. If $i \neq 1$, we have the process under $k-1$ localities in P'_1 and in $k-i < k-1$ localities in Q'_i, with $P'_i \dot{\sim}_l Q'_i$: contradiction. Hence we have $i = 1$, $P_1 \dot{\sim}_l Q' = Q_1$ and $P'_1 \dot{\sim}_l Q'_1$. By induction on $1 \leq j \leq k$, we have $P_j \dot{\sim}_l Q_j$ and $P'_k \equiv n.\mathbf{0} \mid P_{k+1} \dot{\sim}_l n.\mathbf{0} \mid Q_{k+1} \equiv Q'_k$. Since the reduction $P'_k \xrightarrow{n} P_{k+1}$ can only be matched $Q'_k \xrightarrow{n} Q_{k+1}$, we have $P_{k+1} \dot{\sim}_l Q_{k+1}$, consequently we have the required result.

□

In the following, we write X_i the i-th occurrence of X in a process P.

Lemma 50. *Let P, Q two open processes such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Let R, R' two closed processes such that $R \dot{\sim}_l R'$. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} = P_n$ is matched by the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\} = Q_n$ (with $P_n \dot{\sim}_l Q_n$). Then we have the relation $P'\{m.n.\mathbf{0}/X\}\{R/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$.*

Proof. By lemma 49, we have two cases to consider:

- Suppose we have $P_n = n.\mathbf{0} \mid P_1$, $Q_n = n.\mathbf{0} \mid Q_1$ with $P_1 \dot{\sim}_l Q_1$. Since $P_1 \dot{\sim}_l Q_1$, $R \dot{\sim}_l R'$ and $\dot{\sim}_l$ is a congruence we have $R \mid P_1 \dot{\sim}_l R' \mid Q_1$ by transitivity, consequently the result holds.
- Suppose we have $P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$ and $Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$ and for all $1 \leq j \leq k+1$, $P_j \dot{\sim}_l Q_j$. Since $P_{k+1} \dot{\sim}_l Q_{k+1}$, $R \dot{\sim}_l R'$, $\dot{\sim}_l$ is a congruence and is transitive, we have $R \mid P_{k+1} \dot{\sim}_l R' \mid Q_{k+1}$. So we have $a_k[R \mid P_{k+1}] \mid P_k \dot{\sim}_l a_k[R' \mid Q_{k+1}] \mid Q_k$. By induction on $1 \leq j \leq k$, we have $a_j[\dots a_k[R \mid P_{k+1}] \mid P_k \dots] \mid P_j \dot{\sim}_l a_j[\dots a_k[R' \mid Q_{k+1}] \mid Q_k \dots] \mid Q_j$, so we have the required result with $j = 1$.

□

Theorem 19 (**Theorem 14**). *Let P, Q two open processes such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. If $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, then for all closed processes R, we have $P\{R/X\} \dot{\sim}_l Q\{R/X\}$*

Proof. We show that the relation $\mathcal{R}= \{(P\{R/X\}, Q\{R/X\}), P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}, m, n \text{ not in } P, Q\}$ is a strong bisimulation. Since the relation is symmetrical, it is enough to prove that it is a simulation. We make a case analysis on the transition from $P\{R/X\}$:

The transition comes only from P. We have $P\{R/X\} \xrightarrow{\alpha} A\{R/X\}$ with $P \xrightarrow{\alpha} A$. Hence we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} A\{m.n.\mathbf{0}/X\}$. We distinguish the three cases for A:

- Process case P'. Since $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} Q'$ and $P'\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q'$. Since m does not occur in P, Q, we have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} Q'$ comes only from Q. Therefore Q' can be written $Q' = Q''\{m.n.\mathbf{0}/X\}$ for some Q'', and we have $Q\{R/X\} \xrightarrow{\alpha} Q''\{R/X\}$. We have $P'\{R/X\}\ \mathcal{R}\ Q''\{R/X\}$, hence the result holds.

- Abstraction case F. Since $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists F' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} F'$ and $(F\{m.n.\mathbf{0}/X\}) \circ T \dot{\sim}_l F' \circ T$ for all processes T. Since the transition is on a higher-order name, we have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} F'$ comes only from Q. Therefore F' can be written $F' = F''\{m.n.\mathbf{0}/X\}$ for some F'', and we have $Q\{R/X\} \xrightarrow{\alpha} F''\{R/X\}$. Since T is a closed process, we have $(F\{R/X\}) \circ T = (F \circ T)\{R/X\}\ \mathcal{R}\ (F'' \circ T)\{R/X\} = (F''\{R/X\}) \circ T$, hence the result holds.

- Concretion case $C = \langle T \rangle S$. Since $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists $C' = \langle T' \rangle S'$ such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} C'$, $T\{m.n.\mathbf{0}/X\} \dot{\sim}_l T'$ and $S\{m.n.\mathbf{0}/X\} \dot{\sim}_l S'$. We have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} C'$ comes only from Q. Therefore T', S' can be written $T' = T''\{m.n.\mathbf{0}/X\}$ and $S' = S''\{m.n.\mathbf{0}/X\}$ for some T'', S'', and we have $Q\{R/X\} \xrightarrow{\alpha} (\langle T'' \rangle S'')\{R/X\}$. We have $T\{R/X\}\ \mathcal{R}\ T''\{R/X\}$ and $S\{R/X\}\ \mathcal{R}\ S''\{R/X\}$, hence the result holds.

The transition comes only from R. A copy of R is in an evaluation context and perform a transition. We write X_i the occurrence of X where the copy of R performs the transition. We have $P\{R/X\} \xrightarrow{\alpha} P'\{R/X\}\{A/X_i\}$ with $R \xrightarrow{\alpha} A$. Since X_i is in an evaluation context, we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$. Since we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists a transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ (an occurrence of X, noted X_j, is in an evaluation context in Q) with $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$. Consequently we have $Q\{R/X\} \xrightarrow{\alpha} Q'\{R/X\}\{A/X_j\}$.

We distinguish three cases for A:

- Process case R'. We have $P'\{m.n.\mathbf{0}/X\}\{R'/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$ by lemma 50, so we have $P'\{R/X\}\{R'/X_i\}\ \mathcal{R}\ Q'\{R/X\}\{R'/X_j\}$ as required.

- Abstraction case F. By lemma 50, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_j\}$ for all T. We have $(P'\{R/X\}\{F/X_i\}) \circ T = P'\{R/X\}\{F \circ T/X_i\} \mathcal{R}\, Q'\{R/X\}\{F \circ T/X_i\} = (Q'\{R/X\}\{F/X_j\}) \circ T$ as required.
- Concretion case $\langle S \rangle T$. By lemma 50, we have $P'\{m.n.\mathbf{0}/X\}\{T/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{T/X_j\}$, so we have $P'\{R/X\}\{T/X_i\} \mathcal{R}\, Q'\{R/X\}\{T/X_j\}$. Moreover we have $S \dot{\sim}_l S$, and since $\dot{\sim}_l \subseteq \mathcal{R}$ (with P, Q closed processes), we have $S \mathcal{R} S$ and $P'\{R/X\}\{T/X_i\} \mathcal{R}\, Q'\{R/X\}\{T/X_j\}$ as required.

A higher-order communication takes place between R and P. A copy of R is in an evaluation context and communicate with a sub-process P' of P. We have two cases to consider.

The first possibility is $R \xrightarrow{a} F$ and $P' \xrightarrow{\overline{a}} \langle T\{R/X\} \rangle S\{R/X\}$ for some a. We have the transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{F \circ (T\{R/X\})\} \mid \mathbb{E}_{3,R}\{S\{R/X\}\}\}$$

for some evaluation contexts $\mathbb{E}_{1,R}, \mathbb{E}_{2,R}, \mathbb{E}_{3,R}$ (the subscript R means that occurrences of X in the context are filled with R). We have

$$P\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{\overline{a}} \langle T\{m.n.\mathbf{0}/X\} \rangle \mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\}$$

so by bisimilarity hypothesis, there exists $T', \mathbb{E}'$ such that we have

$$Q\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{\overline{a}} \langle T'\{m.n.\mathbf{0}/X\} \rangle \mathbb{E}'_{m.n.\mathbf{0}}\{n.\mathbf{0}\}$$

and the messages and continuations are bisimilar, i.e. we have

$$T\{m.n.\mathbf{0}/X\} \dot{\sim}_l T'\{m.n.\mathbf{0}/X\}$$

and

$$\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\} \dot{\sim}_l \mathbb{E}'_{m.n.\mathbf{0}}\{n.\mathbf{0}\}$$

From the relation on messages, we have

$$F \circ (T\{m.n.\mathbf{0}/X\}) \dot{\sim}_l F \circ (T'\{m.n.\mathbf{0}/X\})$$

Hence by lemma 50 and the relation on continuations, we have

$$\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{F \circ (T\{m.n.\mathbf{0}/X\})\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\} \dot{\sim}_l \mathbb{E}'_{m.n.\mathbf{0}}\{F \circ (T'\{m.n.\mathbf{0}/X\})\}$$

We have $Q\{R/X\} \xrightarrow{\tau} \mathbb{E}'_R\{F \circ (T'\{R/X\})\}$ and

$$\mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{F \circ (T\{R/X\})\} \mid \mathbb{E}_{3,R}\{S\{R/X\}\}\} \mathcal{R}\, \mathbb{E}'_R\{F \circ (T'\{R/X\})\}$$

hence the result holds.

The second possibility is $R \xrightarrow{\overline{a}} \langle T \rangle S$ and $P' \xrightarrow{a} F\{R/X\}$ for some a. We have the transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{S\} \mid \mathbb{E}_{3,R}\{(F\{R/X\}) \circ T\}\}$$

for some evaluation contexts $\mathbb{E}_{1,R}, \mathbb{E}_{2,R}, \mathbb{E}_{3,R}$. We have the transitions

$$P\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{a} \mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{F\{m.n.\mathbf{0}/X\}\}\}$$

so there exists F' such that

$$Q\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{a} \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{F'\{m.n.\mathbf{0}/X\}\}\}$$

for some contexts and we have

$$\begin{aligned}\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{(F\{m.n.\mathbf{0}/X\}) \circ T\}\} \\ \dot{\sim}_l \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{(F'\{m.n.\mathbf{0}/X\}) \circ T\}\}\end{aligned}$$

By lemma 50, we have the relation

$$\begin{aligned}\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{S\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{(F\{m.n.\mathbf{0}/X\}) \circ T\}\} \\ \dot{\sim}_l \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{S\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{(F'\{m.n.\mathbf{0}/X\}) \circ T\}\}\end{aligned}$$

We have $Q\{R/X\} \xrightarrow{\tau} \mathbb{E}'_{1,R}\{\mathbb{E}'_{2,R}\{S\} \mid \mathbb{E}'_{3,R}\{(F'\{R/X\}) \circ T\}\}$ and

$$\begin{aligned}\mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{S\} \mid \mathbb{E}_{3,R}\{(F\{R/X\}) \circ T\}\} \\ \mathcal{R}\ \mathbb{E}'_{1,R}\{\mathbb{E}'_{2,R}\{S\} \mid \mathbb{E}'_{3,R}\{(F'\{R/X\}) \circ T\}\}\end{aligned}$$

hence the result holds.

A higher-order communication takes place between two copies of R. Two copies of R are in evaluation contexts and communicate. There exists $F, \langle T \rangle S$ such that $R \xrightarrow{a} F$ and $R \xrightarrow{\overline{a}} \langle T \rangle S$ for some a. We note X_i, X_j the two occurrences of X in P where the transitions are performed: the transition can be written $P\{R/X\} \xrightarrow{\tau} P''\{R/X\}\{F \circ T/X_i\}\{S/X_j\}$.

We have $P\{R/X\} \xrightarrow{a} P'\{R/X\}\{F/X_i\}$. Since X_i is in an evaluation context, we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$, so there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_k\}$ and $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_k\}$. Since $F \circ T \sim_l F \circ T$, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}$ by lemma 50.

Since X_j is in an execution context, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \xrightarrow{m} P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{n.\mathbf{0}/X_j\}$. Consequently by the previous equivalence there exists Q'' such that $Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\} \xrightarrow{m} Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{n.\mathbf{0}/X_l\}$ and $P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{n.\mathbf{0}/X_j\} \sim_l Q''\{m.n.\mathbf{0}/X\}\{F \circ$

$T/X_k\}\{n.\mathbf{0}/X_l\}$. Since $S \dot{\sim}_l S$, by lemma 50 we have $P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{S/X_j\} \sim_l Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{S/X_l\}$. We have $Q\{R/X\} \xrightarrow{\tau} Q''\{R/X\}\{F \circ T/X_k\}\{S/X_l\}$ and the relation $P''\{R/X\}\{F \circ T/X_i\}\{S/X_j\}\ \mathcal{R}\ Q''\{R/X\}\{F \circ T/X_k\}\{S/X_l\}$, hence the result holds.

□